ICT for peace FOUNDATION

网络政策

进展概要

与信息通信技术相关进程&大事的基本回顾

——对国际和地区安全的影响

（2011-2013）

作者： 卡米诺·卡瓦纳（Camino Kavanagh）

蒂姆·毛瑞尔（Tim Maurer）

艾妮肯·提克-瑞格斯（Eneken Tikk-Ringas）

信息通信技术和平基金会

2014 年•日内瓦

信息通信技术和平基金会，日内瓦。
您可在 www.ict4peace.org 获得手册电子版

与信息通信技术相关进程&大事的基本回顾
——对国际和地区安全的影响
（2011-2013）

作者： 卡米诺·卡瓦纳（Camino Kavanagh）

蒂姆·毛瑞尔（Tim Maurer）

艾妮肯·提克-瑞格斯（Eneken Tikk-Ringas）

目录

缩略词列表

ARF	东盟地区论坛
ASEAN	东南亚国家联盟，简称东盟
AU	非洲联盟
CBMs	建立信任措施
CFSP	共同外交和安全政策（欧盟）
CCDCOE	卓越网络防御合作中心（北约）
CERT	计算机应急响应小组
CHMS	成员国元首理事会（上海合作组织）
CIS	独联体
CNO	计算机网络作战
CoE	欧洲理事会
CSTD	科学与技术促进发展委员会（联合国）
CSTO	集体安全条约组织
DNS	域名系统
ECOSOC	经济及社会理事会（联合国）
ECOWAS	西非国家经济共同体
EDA	欧洲防务局
EMC	欧盟军事委员会
EU	欧盟
GCA	全球网络安全议程（国际电信联盟）
GCHQ	英国政府通信总部
GGE	政府专家组（联合国）
IANA	互联网数字分配机构
ICANN	互联网名称和数字地址分配机构
ICTs	信息通信技术
IGF	互联网治理论坛
ITU	国际电信联盟
LDCs	欠发达国家
MDGs	千年发展目标
MOU	谅解备忘录
NATO	北大西洋公约组织
NRRCs	核风险减缩中心
NSA	国家安全局（美国）
NTIA	国家通信与信息管理局（美国商务部）
OAS	美洲国家组织
OECD	经济合作与发展组织
OSCE	欧洲安全与合作组织

PC	常任理事会（欧安组织）
SADC	南部非洲发展共同体
SCO	上海合作组织
UN	联合国
UNCTTF	联合反恐执行工作队
UNODC	联合国毒品与犯罪问题办公室
WCIT	国际电信世界大会
WSIS	信息社会世界峰会

关于作者

卡米诺·卡瓦纳，目前正在伦敦国王学院战争研究系攻读博士学位，研究重点是网络空间及战略转型。她现任信息通信技术和平基金会和美国外交政策全国委员会（NCAFP）的高级顾问，并负责召集年度“网络安全与美国外交政策”圆桌会议。她有 15 年在爆发冲突和冲突后地区工作的专业经历，现往返于纽约、马里首都巴马科和伦敦之间，定期为国际组织和政府机构提供咨询。

蒂姆·毛瑞尔，新美国开放技术研究所研究员，他关注网络空间和国际事务，包括网络安全、互联网自由和互联网治理。 2013 年 10 月和 2014 年 2 月，他曾在联合国就网络战发表演讲，他的研究成果也由哈佛大学、《外交政策》杂志、美国有线新闻网（CNN）及知名网络杂志 Slate 等刊登发表。

艾妮肯·提克-瑞格斯博士，是英国国际战略研究所网络安全资深研究员，关注网络空间国家力量的运用及与国际网络安全相关的法律和政策问题。她现任波罗的海防务学院网络安全高级专家。并自 2011 年开始向信息通信技术和平基金会理事会提供国际网络安全方面的咨询。

关于信息通信技术和平基金会

信息通信技术和平基金会（网址 www.ict4peace.org），肇创于 2003 年日内瓦召开的联合国信息社会世界峰会（WSIS），旨在通过更好的理解和运用 ICT，促进政府、民众、社会团体和利益相关方开展有效

和持续的沟通，更好地预防冲突、调解矛盾与维护和平。本基金会的“网络空间权利与安全”项目始于 2011 年。我们志在跟进、支持和领导双边及多边的外交、法律和政策行动，努力构建一个安全、繁荣和开放的网络空间。基金会的出版物可在 http://ict4peace.org/?p=1076 查找，主要包括：

- 着手实施：促进网络空间和平的现实目标（2011）
- ICT4Peace 关于即将在纽约召开的联合国网络安全政府专家组会议（GGE）的简报（2012）。
- 对全球和地区进展、议程和措施的概述（2013）
- 下一步干什么？网络空间信任措施建立（2013）
- 获取应对国际网络安全挑战的软实力（2013）

致　谢

作者感谢信息通信技术和平基金会总裁丹尼尔·斯道法赫，感谢他在写作过程中提供的宝贵意见及给予作者的宽容耐心。特别感谢罗伯特·毛格斯在报告起草过程中给予的出色研究支持。罗伯特是新美国开放技术研究所的一位研究助理，他主要研究互联网治理，国际网络安全和网络人权。

作者在此还要特别感谢伊万·布坎南（联合国“发展援助”机构），罗恩·迪波特教授（多伦多大学公民实验室），詹姆斯·刘易斯（美国战略与国际研究中心），保罗·梅耶（加拿大西蒙·弗雷泽大学），内曼加·马里塞维奇（原在欧安组织任职，现供职于微软）和史国力（美国对外关系委员会），感谢他们在报告撰写的各阶段提出的精彩意见和建议。该研究报告于 2014 年 3 月完成。

国际和地区安全领域
与信息通信技术相关的进程&大事的基本回顾
（2011-2013）

1、背景&介绍

鉴于计算机系统和相关技术的脆弱性及恶意使用，各国的不安全感日益强烈。因此，过去五年来，各国越来越多地就“网络安全”的地区和国际政策问题展开讨论。自 20 世纪 80 年代开始，此环境下的脆弱性和威胁就有所呈现，各国和各非国家行为体均发展出了应对它们的创新方法和手段。[1]然而，仅在近五到七年时间里，网络威胁和脆弱性才上升至政治和战略高度，直接（并经常是充满过度热情的）进入国家、地区和国际安全议程。[2]

当前各国对“网络安全”日趋关注缘于全球战略环境的重大改变：中国作为全球经济和地区军事大国的崛起；全球金融危机及其仍在发酵的影响；崛起中的中等收入国家参与国际和地区政治事务的信心增强。这些变化增大了国际环境的不确定性，使得围绕“网络空间”和通过 ICTs 谋求政治、军事和经济优势的讨论更加复杂。近来，ICTs 在中东和北非政治剧变中发挥作用，一些国家被指使用尖端恶意软件实现外交政策目标，爱德华·斯诺登曝光由美国国家安全局和英国政

[1] 马立安姆·邓恩－卡维尔蒂（Myriam Dunn-Cavelty），维克多·毛瑞尔（Victor Mauer）和塞·弗利西亚·克里申娜－汉恩斯（Sai Felicia Krishna-Hense）编辑：《信息时代的实力和安全：调查国家在网络空间的角色》，英国阿什盖特出版社(2007)。

[2] 《网络索引：国际安全趋势和分析（2013）》，CSIS（美国国际与战略研究中心），IPRSP，联合国裁军研究所（UNIDIR），参见： http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf。

府通信总部主导的大规模网络监控行为等，不经意间引发了各国进一步介入的兴趣。

尽管国际和地区论坛对这些关切有所回应，但 2013 年以前的所有议程并未就此取得一致。事实上，2012 年 12 月在迪拜举行的国际电信世界大会（WCIT）充分表明了各国对于如何治理互联网存在重大分歧，互联网治理问题与国家、国际网络安全关切越来越交织在一起。[3]WCIT 大会还证实，不同国家对网络空间特别是“互联网”持不同看法，它们间的地缘政治鸿沟不断扩大：一方支持一个开放、自下而上的 ICT 环境或符合民主价值观的“网络空间”，另一方则支持一个封闭的、自上而下的，国家主导的，受国家主权和不干涉原则保护的“信息环境”。[4]

尽管如此，2013 年还是取得了一些积极进展，如在联合国和欧安组织框架下，就国际法和其他现有国际规范与原则适用于网络空间、建立信任措施和能力建设措施等达成的多边协议。俄罗斯和美国就建立信任措施签订双边协议，其他地区和双边进程的启动也释放了积极信号。

2013 年首尔网络空间会议期间，信息通信技术和平基金会主持了一个分会，以确保现存以及新兴的网络安全相关议程更具包容性为重点，吸纳更多的地区、公民社会、产业界和学术界参与讨论（这

[3] 丹尼尔·凯尔（Danielle Kehl）和蒂姆·毛瑞尔(2012)：“国际电信世界大会 2012 业已结束”，参见：http://www.slate.com/blogs/future_tense/2012/12/14/wcit_2012_has_ended_did_the_u_n_internet_governance_summit_accomplish_anything.html；丹尼尔·凯尔和蒂姆·毛瑞尔(2012)：“WCIT2012： 峰会一半时间用来分析如何打造互联网的未来”，参见：http://www.slate.com/blogs/future_tense/2012/12/11/wcit_2012_a_half_time_analysis_of_the_itu_summit_on_internet_governance.html

[4] 蒂姆·毛瑞尔和罗伯特·莫格斯（Robert Morgus），“国际治理创新中心”（CIGI）互联网治理系列报告（即将出版）。

是对 2013 年联合国政府专家组报告的响应）。基金会的会议声明重申上述观点，努力使有关网络安全问题各种进展的信息能传递到更广泛地区，并采取一些措施把它们传递给政府。[5] 本报告是朝此方向努力的第一步。

本报告由以下三部分构成：一是国际和地区安全（主要焦点）；二是跨国犯罪和恐怖主义；三是治理、人权和发展。这些问题范畴显然彼此关联，一个领域的发展往往会影响到其他方面。然而近 15 年来，它们却往往由不同的团体和论坛进行实践与探讨。最新进展表明，上述领域正在不断融合，一方面为制定更广泛的协议提供了契机，但另一方面也增大了出现更多误解和张力的风险。本报告将作为未来年度报告的基础，时间跨度为 2011 年 1 月至 2013 年 12 月。此外，报告还关注了 2014 年度重要的政策事件和进程。

最后，作者在本报告中谨慎使用“网络空间”和“网络安全”术语，因为有关这些定义的很多重大挑战仍未解决。[6] 在西方，政策界通常使用“网络空间”和“网络安全”概念。而包括上合组织成员在内的其他国家则继续使用“信息空间”或“信息环境”概念。定义的分歧和不时被混用的状况，反应了各方对当前问题明显不同而又高度功利性的解读。尽管各国日益有意参与有关网络安全议题的讨论，但如果基本定义和概念不能达成一致，实际进展将很难取得。

[5]《信息通信技术和平基金会会议报告》，首尔网络空间会议声明，参见 http://ict4peace.org/seoul-conference-on-cyberspace-2013-statement-on-ict4peace-special-session/.
英国政府对首尔网络空间会议贡献的报告，参见 https://www.gov.uk/government/publications/uk-contribution-to-the-seoul-conference-on-cyberspace

[6]凯尔·吉尔斯（Keir Giles）和威廉·哈格斯塔德（William Hagestad）(2012)：通用语言的分歧：汉语、俄语和英语的网络定义》，2013 年第 5 届网络冲突国际会议报告，北约卓越协作网络防御中心。

2、国际与地区安全

2.1 国际安全

2000 年以来，越来越多的国家将网络安全或信息安全纳入国家安全议程，投入大量资源来提升应对网络威胁和脆弱性的国家能力、制订网络军事行动准则、发展攻防能力。[7]各类通过网络能力在战场上获取政治目标的报道、国家争相制订军事网络战略和发展恶意 ICT 能力的现实，迫使各国开始共同探讨：如何将网络能力发展置于现行国际法管辖之下？如何限制国家使用此类能力？

1998 年，俄罗斯向联合国大会负责裁军和国际安全事务的第一委员会提交了一份决议草案，回应美军的信息控制和信息战学说。[8]自此，联合国开始探讨信息通信技术的不当使用及其可能带来的国际安全风险。随后连续三届联合国信息安全专家组（UN GGE）均受命从国际安全角度就信息和电信领域的发展展开讨论。[9]2012 年，依据联合国 A/Res/66/24 号决议，第三届信息安全专家组成立并于 2013 夏季发布了工作报告。尽管成员观点有相当程度的分歧，信息安全专家组还是就规则、信任和能力建设措施等系列议题达成了共识。此外，专家组报告还确认，“国际法，特别是《联合国宪章》适用于各

[7] 《网络索引：国际安全趋势分析》（2013），CSIS、IPRSP、UNIDIR。http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf。

[8] 参阅克鲁斯金赫（Krutskikh）等编（2009）:《国际信息安全：和平外交》，莫斯科。尤其参阅科莫夫（Komov）文章，“论现代美国信息战学说的演进”。

[9] 尽管得到少数国家支持，俄罗斯早期的决议草案并未获得广泛认同。2009 年，美国最终决定参与网络空间国家行为规则探讨，形势自此发生变化。2010 年，联合国大会第一委员会的联合国专家组（UNGGE）举行了关于“建立全球网络安全文化”系列会议，首次就某些措施取得一致。2011 年 12 月，联大同意建立新的专家组来推动措施实施并“继续研究信息安全现有和潜在的威胁以及应对威胁的合作手段，包括国家负责任行为的规范、信息空间建立信任措施等。”参阅蒂姆·毛瑞尔（2012）：“联合国制订网络规则：联合国网络安全活动分析”，贝尔弗科学与国际事务中心；艾妮肯·提格－瑞格斯（2012）：“国际安全视角下的信息与电信发展：1998－2012 年的联合国第一委员会工作”，ICT 4 Peace。

国使用信通技术，对维持和平与稳定及促进创造开放、安全、和平和无障碍信通技术环境至关重要。”[10] 专家组也同意，“国家主权和源自主权的国际规范和原则适用于国家进行的信通技术活动，以及国家在其领土内对信通技术基础设施的管辖”。[11] 报告还强调，各国在努力处理信通技术安全问题的同时，必须尊重《世界人权宣言》和其他国际文书所载的人权和基本自由。[12]

考虑到此前 GGE 和其他相关进程所遭遇的困难（第一届专家组未达成任何共识），2013 年 GGE 报告可谓一个巨大进步。例如，2011 年 9 月，俄罗斯、中国等国在第 66 届联合国大会上散发了《信息安全国际行为准则》（以下简称《准则》），声称（西方国家造成的）日益增长的互联网军事化是促使他们提交此《准则》的原因。[13]《准则》得到上海合作组织（SCO）强力支持，SCO 称其为“第一份相对全面的信息和网络安全国际准则”。该文件与《国际人权宣言》类似，目的是要建设“和平、安全、开放与合作的网络空间。”[14] 由于始终不

[10] 《从国际安全的角度来看信息和电信领域发展政府专家组报告》（A/68/98），第三部分“关于国家负责任行为的规范、规则和原则的建议”（第 19 段），
http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=E 。

[11] 同上（第 20 段）。

[12] 同上（第 21 段）。其它共识包括：各国应在打击犯罪或恐怖分子使用信通技术方面加强合作，酌情协调法律办法，并加强各自执法和检察机关的实际协作；各国必须履行对应归咎他们的国际不法行为的国际义务，而且不得使用代理人实施此类行为。各国应设法确保其领土不被非国家行为体用于非法使用信通技术。在第四、第五部分，报告列举了一系列“建立信任措施”，以“自愿建立信任措施可促进各国间的信任和信心，有助于通过提高可预见性和减少误解降低冲突风险”；能力建设方面，“加强关键信通技术基础设施安全；发展技能并拟订适当立法、战略和监管框架，以履行职责；弥合信通技术安全及其使用方面的鸿沟。”通过推行报告所建议的能力建设措施，ICT 安全性将会提升，有助于实现“建立促进发展的全球伙伴关系” 的“全球千年发展目标 8”。需要注意的是，GGE 报告认识到非国家行为体——尤其是私人部门、学术界和公民社会——在协助 GGE 措施落实中发挥重要作用。

[13] 《行为准则》由中国、俄罗斯、塔吉克斯坦、乌兹别克斯坦常驻联合国代表提出（A/66/359）。

[14] “中国、俄罗斯等国向联合国《信息安全国际行为准则》”，中华人民共和国外交部，见 http://www.fmprc.gov.cn/eng/wjdt/wshd/t858978.htm，同时见 C・捷佐塞克（C. Czosseck）、R・奥提斯（R.Ottis）和 K・齐奥克沃斯基（K. Ziolkowski）编：《第四届国际网络冲突大会汇编》，2012 年，北约卓越协作网络防御中心出版。

接受西方国家将现有武装冲突法律适用于“信息空间”的倡导，中、俄及其它 SCO 成员国提出此份《准则》作为替代方案。2011 年，在叶卡捷林堡“第二届国际安全事务高官会议”上，俄罗斯抛出《国际信息安全公约》构想，进一步明确其立场。[15] 俄通过在系列高层会议宣传公约的好处，最终获得 近52 个国家的支持。

《准则》和公约草案都包括禁止将互联网用于军事目的和颠覆它国政权的自愿性条款，也暗含要应对西方利用信息通信技术实施文化渗透和谋求军事优势的威胁。接受草案条款将确保各国拥有制定网络空间政策的主权；此外，两个文件虽都包含言论自由和信息获取权的条款，但这些权利均要服从国家安全规定。诚如俄罗斯信息安全专家安德烈·克鲁斯金赫（Andrey Krutskikh）所言，“确保信息安全决不能压制自由，推行自由决不能危及国家安全和主权”。[16] 2009 年的 SCO《保障国际信息安全政府间合作协议》以及一些影响独联体（CIS）国家高层 ICT 战略、政策的协议均具有类似条款。震网等重大安全事件、社交媒体在阿拉伯地区政治动荡中的重要作用更加强化了上述论调。然而，2013 年 6 月的 GGE 报告也确实显示一些国家改变了立场。2013 年英国举办的八国集团（G8）外长会议上，这种立场转变再次得到印证，八国外长（包括俄罗斯）确认“如同现实空间一样，国际法适用于数字世界”，强调“必须采取措施推动透明和信任建设以降低国家间误判的风险。”[17] GGE 报告中“国际法适用于网络空间”论

[15] 《国际信息安全公约》，2011 年 11 月 28 日，http://rusemb.org.uk/policycontact/52。
[16] 俄罗斯外交部代表克鲁斯金赫在“伦敦网络空间国际会议”上的发言，2011 年 11 月。
[17] https://www.gov.uk/government/news/g8-foreign-ministers-meeting-statement 。

断是美等西方国家的主要外交目标，因此被这些国家视为“成果”。同样，中、俄也得到了类似“成果”，即 GGE 报告接受了主权原则。但是，这些“成果”“马上受到两大问题制约，即这些原则如何适用于国家行为仍待进一步研究，未来还应制订其它更加符合 ICTs 特点的规则。”[18]

按照俄罗斯 2013 年 12 月的提议，2014 年将建立一个新的 GGE，成员由 15 个扩充到 20 个，增加了南半球国家的数量。[19] 新 GGE 的目标是继续讨论 2013 年报告中已取得共识的议题。[20] 关键问题是就现有国际准则下可接受的国家行为达成一致。另外，网络空间何种行为构成使用武力亦有待形成共识。网络空间武力攻击行为的界定、网络自卫使用的时机（联合国宪章 51 条规定），特别是军事必要、比例原则适用等，都是十分棘手的问题。但需要指出的是，越来越多的专家们同意：单纯的“网络”武装冲突存在的可能性很小；网络能力会更多地被用于现实武装冲突以获取军事和政治“效果”，因此，应从这个角度来探讨。[21]

美国、英国大规模电子监控行为的曝光也可能对下届 GGE 工作产

[18] 保罗·迈耶尔（Paul Meyer）：“网络空间信任建立：联合国专家同意这是个好办法”，2013，加拿大国际委员会，见 http://opencanada.org/features/the-think-tank/comments/confidence-building-in-cyberspace/ 。

[19] 新一届 GGE 的成员国将包括：5 个安理会常任理事国、安提瓜和巴巴多斯、白俄罗斯、巴西、哥伦比亚、埃及、爱沙尼亚、德国、加纳、以色列、日本、肯尼亚、马来西亚、巴基斯坦、韩国和西班牙。主席国尚未确定。

[20] 俄罗斯在本年度联大提出决议草案，呼吁在 2014 年建立新一届 GGE，继续探讨相关议题。成员国表示同意，关于成立时间、成员构成、成员数量（15 个还是 20 个）等议题则正在议定之中。

[21] 同样值得指出的是，有关人道主义法是否适用于冲突中的技术使用（尤其是无人飞行器）的讨论使得网络空间和国际安全争论已扩展到更广泛的领域。虽然尚不清楚如何与当前国际安全视角下的信息和电信探讨相联系，但关于无人机的讨论将可能成为下一届联大的议题。巴基斯坦推动将无人飞行器使用纳入联合国人权理事会议程（置于委员会反恐工作框架下），此举激起一定反响，尤其受到美国抵制，美国认为人权理事会不是探讨此类议题的恰当平台。参阅 NCAFP 圆桌进程，网络安全，美国外交政策、正在改变的局面以及最近发表的《联合国人权理事会不是讨论无人机的恰当平台：美国论巴基斯坦的提议》，First Post,2014 年 3 月 21 日（www.firstpost.com/world/unhrc）等文章。

生影响。长期以来，经济、政治间谍活动议题主要在双边层面处理；然而联合国大会近来已然成为回应此类关切的平台，联大下设的各委员会有关 ICTs 的讨论则越来越类似甚至重叠。美国家安全局监控德国、巴西领导人的间谍活动曝光后，巴西总统罗塞夫在纽约 2013 年联大开幕式上对此进行了激烈批评。[22] 讲话后，德国、巴西共同向联大第三委员会（负责人权事务）提交了一份关于“数字时代隐私权”的决议草案，2013 年 12 月 18 日此草案未经投票而获得通过。[23] 2014 年 4 月，巴西在圣保罗举办了 NetMundial 大会（容后详述）。

其它

2007 年，国际电信联盟（ITU）设立“全球网络安全议程（GCA）”，以此作为成员国应对网络安全挑战的合作框架。[24]

2013 年初，信息社会世界峰会（WSIS）（第 5 部分将进行详细讨论）通过的《原则宣言》关注不同安全议题，包括“在 ICT 使用中建立信任与安全”[25]，后者在《日内瓦行动计划》中有所体现[26]。2005 年，依据 WSIS《突尼斯承诺》，政府承诺利用 ICT 促进和平、避免冲

[22] 巴西联邦共和国总统迪尔玛·罗塞夫阁下在第 68 届联大一般性辩论会开幕式上的讲话，纽约，2013 年 9 月 24 日，http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf 。

[23] 有意思的是，与此同时，77 国集团和中国向联合国第二委员会（经济与财政委员会）提交了一份关于 ICT 促进发展的决议草案（9A/C.2/68/L.40），其中出现了“未授权的非法拦截”语句并要求联合国秘书长就此出台相关报告。由于遭到反对且巴西、德国的联合提案已经提及此议题，2013 年 12 月 18 日最终通过的联合国决议（A/68/167）删除了上述语句。决议见：
http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167&referer=http://www.un.org/depts/dhl/resguide/r68_en.shtml&Lang=E

[24] 2007 年 ITU 成员国通过了《全球网络安全议程》，此议程关注法律措施、技术与程序措施、组织架构能力建设及国际合作。

[25] 参阅《建设信息社会：新千年的全球挑战》，第 B5 部分，“树立使用 ICT 的信心并提高安全性”，尤其是第 35-37 段有关建立信任框架；避免将 ICT 用于与维护国际稳定与安全宗旨相悖的目的；在相应的国家层面和国际层面解决垃圾邮件，http://www.itu.int/wsis/docs/geneva/official/dop.html

[26] 见《日内瓦行动计划》，第 C5 条：“树立使用 ICT 的信心并提高安全性”。
http://www.itu.int/wsis/docs/geneva/official/poa.html

突。[27]2013 年，国际电联和联大发起 WSIS 评估进程，对日内瓦和突尼斯“原则宣言”、“行动计划”和“承诺”中有关安全内容进行总体评估。

除了正式多边进程外，2011 年 11 月，英国政府发起了之后演变为年度大会的系列国际会议—“伦敦网络空间国际会议”。会议的创办宗旨在于聚集各利益攸关方—尤其是志同道合的国家—共同探讨广泛的网络议题，尤其网络安全议题。伦敦会议开创以来，英国政府提出了一系列网络空间原则，[28]匈牙利（2012）和韩国（2013）先后接捧承办了后续会议。“首尔会议”通过了名为“一个开放和安全网络空间的框架”报告。[29] 虽然一些人认为伦敦会议首要关注网络安全问题，但会议不断拓展其讨论的领域，进而带来了如何与其他论坛（如那些关注互联网治理问题的平台）互动的问题。

2.2 地区安全

与国际层面的GGE 工作同步，各国也已在地区论坛中讨论对网络安全的关切。[30]一些进程取得了积极进展，促使国际社会对国家合作意愿、战略性限制使用 ICT 实现政治目的等前景保持些许乐观。

[27] 《突尼斯承诺》第 36 段：“我们珍视 ICT 在促进和平和避免尤其不利于实现发展目标的冲突方面所具有的潜力。ICT 可以通过预防冲突的早期预警系统确定冲突状况，从而促进冲突的和平解决、支持人道主义行动，包括向武装冲突中的平民提供保护、协助执行维和任务，并协助开展冲突后的和平建设和重建工作。http://www.itu.int/wsis/docs2/tunis/off/7.html。2004 年，瑞士和突尼斯政府将第 36 段作为外交谈判的立场，以推动其成为 2005 年《突尼斯承诺》的一部分。2006 年春，ICT4Peace 成立，激发世人关注《突尼斯承诺》，推动其切实应用于危机管理的各阶段。

[28] 见注释 111。

[29] “首尔网络空间大会”相关信息见 http://www.seoulcyber2013.kr/en/about/meeting.html。

[30] 见 ICT4Peace 报告及 CBM 的状态模型（2014 年 2 月更新），http://ict4peace.org/what-next-building-confidence-measures-for-the-cyberspace/

2.2.1 欧洲安全与合作组织（OSCE）

例如，2013 年 12 月，OSCE 常设委员会通过第 1106 号决定，出台“OSCE 降低 ICT 使用导致冲突风险的初步建立信任措施（CBMs）”。[31] 这套 CBMs 聚焦于若干重要的透明化措施，有利于各层面的信息交换和沟通。

这套 CBMs 特别包括各种自愿性承诺：如分享各国对 ICTs 应用带来的国家、国际威胁的看法；促进国家间合作、交换 ICTs 使用及安全方面的信息；加强协商以减少误解，降低 ICTs 使用可能导致的政治、军事冲突等风险；保护国内、国际关键 ICT 基础设施（含完整性）；分享确保互联网开放、共享、安全和可信的措施。[32] 由于之前试图达成协议的努力未能成功，OSCE 此份 CBMs 协议意义重大。同样重要的是，从一开始，OSCE 的 CBMs 就被作为其它地区或国际组织相关进程的有益借鉴，如 GGE 和东盟地区论坛等。

然而，OSCE 于 2013 年达成的 CBMs 协议主要基于自愿，其中缺乏监督和审查措施，因而落实情况无从知晓。但无论如何，此份开创性的 CBMs 可看做是 OSCE 成员国友好愿望的表达，纵然许多工作仍待完成，但它不失为过去几年此领域最积极的进展。

2.2.2 北大西洋公约组织（NATO）

北约早就重点关注网络安全和网络空间问题。在作战层面，北约

[31] OSCE：“OSCE 降低 ICT 使用导致冲突风险的初步建立信任措施”，2013 年 12 月 3 日，PC.DEC/1106。见 http://www.osce.org/pc/109168?download=true。
[32] http://www.osce.org/pc/109168

将“网络防御”整合进“防御规划进程（NDPP）”，此进程“提供了一个框架，是协调成员国及联盟防御规划的重要工具”。[33]2002 年来，网络防御几乎被纳入所有北约峰会议程并不断受到高层重视。但 28 个成员国间参差不齐的网络安全能力和国家政策却成为实现共同防御的障碍。

2012 年芝加哥峰会强调，北约需要与联合国、欧盟和欧安组织等建立伙伴关系。为此，北约将推进成员国发展国家网络防御能力，包括强化成员国自身的能力，组织和支持沟通，培训、教育和演习，分享信息和最优做法，推进协同能力发展进程与项目。[34]

2007 年爱沙尼亚遭受网络攻击后，北约通过签署国家间网络防御合作与协调备忘录主动强化网络防御。预计 2014 年 9 月威尔士峰会召开之际，所有北约成员都将签订类似备忘录，备忘录模板将根据届时提交给威尔士峰会审议的新政策进行更新。[35] 同时，北约与伙伴国的努力还包括：系列跨国试点活动以及与乌克兰进行网络防御专家对话。2014 年，北约将举办一系列与网络安全相关的 CBMs 和规则会议。

2013 年，北约授权的独立智库“北约卓越合作网络防御中心（CCDCOE)”发布《国际法适用于网络空间的塔林手册》。受 CCDCOE

[33] G8 外长会议声明“跨国挑战和机遇”部分，
https://www.gov.uk/government/news/g8-foreign-ministers-meeting-statement。
[34] 2013 年 10 月底，通信与信息局（NCIA）宣布北约“计算机事故响应能力（NCIRC）”具备了“全面运 行能力（FOC）”，这被视为北约增强网络防御的一个里程碑。北约仍将不断完善、升级这一能力，重点是 保护北约自身网络并提升整个联盟的防御水平。因此，NCIRC FOC 不是一个目标，而是一个长期的承诺和进程。近期，北约不会发展网络进攻能力，但“联盟作战司令部（ACO）”对网络作战很热衷。基于整体考虑，网络防御被作为作战规划和作战实施的一部分，与各种威胁（能源、恐怖主义和网络）和响应机制（北 约、国家）结合起来。2012 年，“联合全面作战与管理中心”（CCOMC）成立，下设了“网络防御小组（CDC）”。
[35] 来自 2014 年 3 月 10 日与北约代表的交谈。

之邀，20 名法律学者和业界人士参与了手册撰写。《塔林手册》探讨了国际人道法及网络冲突中“诉诸战争权”的适用问题，提出了一系列定义，包括最受争议的“网络攻击”。专家组反对将网络空间视为需独创一个法律体系的特殊领域。但实践也证明，国际法准则在网络空间的适用面临诸多挑战，最突出的例子便是专家们难以就国际法所定义的“攻击”如何适用于网络作战达成共识。[36] 专家组也发现，“如同适用于陆海空一样，将国际法应用于网络空间同样会引发众多争议”，如关于“战 争支撑”军事行动的争论。[37] 虽然专家组提出的国际法适用网络空间的论点引发了一些法律和政治争论，[38] 但《塔林手册》推动了对这一问题的探讨。

2.2.3 欧盟（EU）

2013 年 2 月，欧盟发表了《网络安全战略》，聚焦于确保互联网开放、有效应对网络恐怖主义和保护关键基础设。[39] 新研究表明，欧盟 2008 年安全战略虽然将“网络威胁”列为该地区面临的新安全威胁，但“共同外交与安全政策”（CFSP）框架下的相关措施进展甚微。[40]2008 年来，欧洲防务局（EDA）和欧盟军事委员会（EMC）就计算机网络作战（CNO）开展了多方面研究；2009 年来，欧盟就集体防御组

36 “网络空间的国际法：高洪柱的讲话与塔林手册”，迈克尔·施密特（Michael·N·Schmitt，2012），《哈佛国际法期刊》（12 月 12 日），第 54 期（在线）。

37 同上。

38 奥利弗·凯斯勒（Oliver Kessler）和沃特尔·威纳（ Wouter Werner）：“专门知识、不确定性和国际法：关于网络战的塔林手册研究”，《林登国际法期刊》，26 卷，第四期，2013 年 12 月，第 793-810 页；迪耶特·弗 莱克（Dieter Fleck）：“寻求适用于网络空间的国际规则—对新塔林手册的第一次关键评估”，《冲突与安全 法期刊》（2013 年夏），18 (2): 331-351。

39 《欧盟网络安全战略：一个开放、安全、可靠的网络空间》，布鲁塞尔，2013 年 2 月 7 日。

40 亚历山大·克林姆伯格（Alexander Klimburg）和赫利·提尔玛·克拉尔（Heli Tirmaa-Klaar）：“网络安全与网络权力：欧盟行动的概念、条件和能力”，欧盟对外政策总署政策部，EXPO/B/SEDE/FWC/2009-01/LOT6/09 PE 433.828 ，2011 年 4月。

织了系列研究，举办研讨会探讨网络安全及欧盟军事机构推动计算机网络作战准则的意义。[41] 尽管“之前已在欧盟战斗组下对‘战术计算机网络作战’这一较狭小的领域进行了探索”，上述努力仍受制于“相对较弱欧盟指挥和控制能力”，拖了本地区建设共同防御力量的后腿。直到现在，重大网络事故响应仍由“理事会安全委员会”（INFOSEC）负责，这是“一个有权但神秘、且主要关注自身信息保障的机构”。[42] 虽然“信息保障”已成为“直接影响欧盟机构当前安全”的重要问题，但它并未得到“共同外交与安全政策”授权，因此，即便发生了国家支持的、针对欧盟机构的网络攻击（这些年媒体报道了很多），它也不用通报给“共同外交与安全”的责任机构。[43]

2.2.4 东盟地区论坛（ARF）

致力于打击恐怖主义和跨国犯罪同时，ARF 也已成为亚洲国家进行国际网络安全探讨的地区平台。2012 年 3 月的一个研讨会主要讨论了代理人或“代表政府的组织和个人对它国政府、私营部门和公民发动恶意网络行动”的问题。[44] 同年 9 月，另一场关于 CBMs 的研讨会特别聚焦了“网络安全法律框架是否欠缺”及“如何制订规则以界定不可接受的国家行为”等议题。[45]

ARF 也成为探讨中、俄“行为准则”价值的平台。[46]2013 年 10 月，

[41] 同上。
[42] 同上。
[43] 同上。
[44] “东盟地区论坛网络空间代理人研讨会联合主席总结报告”，越南，会安市，2012 年 3 月 15 日。
[45] “东盟地区论坛网络空间建立信任措施研讨会联合主席总结报告”，韩国，首尔，2012 年 9 月 12 日。第 8 点。
[46] 同上，第 19 和 23 点。

中国与马来西亚共同主办 ARF“强化网络安全措施——法律和文化的视野”研讨会。[47]这一年，ARF 成为中国、日本、美国与东盟国家探讨网络空间建立信任措施的双边平台。[48]出于议题的急迫性，2014 年 3 月，马来西亚和澳大利亚在吉隆坡共同主办了第二次 ARF 研讨会，有意突出“行动导向”，旨在就亚太地区网络安全领域建立信任的具体措施达成共识。[49]吉隆坡会议取得三个核心成果：1）确定了各国相应的联络点并同意在未来数月或数年内保持不变；2）明确了对东盟各国网络协调和技术能力的基本要求；3）确保未来 CBM 程序中延续本次会议采取的桌面推演形式。[50]

2.2.5 上海合作组织(SCO)，集体安全条约组织(CSTO)，独联体(CIS)

在其它地区，上海合作组织、集体安全条约组织和独联体提出了《行为准则》与《国际信息安全公约构想》，上述组织成员国仍大力推进两份文件提出的相关原则。例如，2012 年北京会议期间，SCO“成员国领导人理事会”（CHMS）重申国家主权和不干涉的承诺，号召推进“和平、安全和开放的信息空间”；同时承诺继续在联合国支持下推广《行为准则》。2013 年 9 月，该理事会发表《比什凯克宣言》，重申上述“尊重国家主权和不干涉它国内政”的原则。[51]

未来 18 个月，国际安全和互联网治理有关进程将着重处理两类

[47] “北京东盟地区论坛研讨会评论”，可参阅 http://aspistrategis.org.au/arf-and -how-to-change-the-tune-of-the-cyber-debate/。
[48] http://csis.org/files/attachments/130723_jimlewis_testimony_v2.pdf。
[49] “第二次东盟地区论坛网络安全研讨会成果概览”可参阅 http://www.aspistategiist.org.au/cyber-confidence-building-in -the-asia-pacific-three-big-take-away-from-the-arf/
[50] 同上。
[51] 上海合作组织成员国领导人理事会《比什凯克宣言》，比什凯克，吉尔吉斯斯坦，2013 年 9 月 13 日。

原则的平衡：一类将国家推至网络安全议题的主导地位；另一类则旨在保护公民、确保数据跨越国界自由流动。

CSTO 和 CIS 尤其针对恐怖分子、犯罪分子利用 ICT 制造威胁等制定了相应措施。

2.2.6 美洲国家组织（OAS）

21 世纪初，网络安全就已被列入 OAS 工作议程。实际上，该地区是最早制订网络安全威胁应对战略的地区。[52]OAS 主要关注：建立打击网络犯罪及其它形式有组织犯罪的共同框架；确保国家具有应对系统脆弱性的能力；确保国家响应工作与 OAS 加强民主治理和地区人权架构的努力相一致。下部分将对此进行详述。

最近，一些 OAS 国家开始把通信、电子和信息战军事准则纳入国防战略框架中。例如巴西《2008 年国防战略》提出了重组军队、 调整国防工业以确保其能向陆海空三军提供国内技术支撑的指导原 则；将“控制论”作为国防政策的一个战略要素；建立“网络战通信 中心”等。[53] 阿根廷军队制订了“通信和电子战联合军事准则”；2009 年来，哥伦比亚一直寻求出台“指导网络空间军队和警察行动的联合 准则”。[54]但 OAS 和其它拉美、加勒比次地区组织均缺乏一套共同应对 网络安全挑战的战略表述，这既说明本地区存在更多迫切需要应对的 问题，[55] 或许也说明美国的影响力在下降，无法施加权威、塑造结果。[56]

[52] AG/RES. 2004(xxxiv-o/04)。
[53] 刘易斯（Lewis）和提姆林（Timlin），2011 年。
[54] 同上。
[55] 尽管 OAS 秘书长将应对多维度安全视为要务，但其核心是“毒品、武器和人口走私导致的严重公共安全危机；洗钱和有组织犯罪。”该组织的其它优先任务包括强化民主治理、提升地区人权制度；调和民主建设

2.2.7 非洲联盟（AU）

同样，非洲联盟应对网络安全威胁和脆弱性的水平还未达到发展地区性军事响应能力的阶段。除本地区武装力量有限外，AU（以及其他次地区组织）的关注重点仍是维和与打击极端主义，短期内这种情况不会有变化。但网络犯罪已经成为核心关切，正如下面即将谈到的，非洲地区正努力制订共同的网络安全战略。

2012 年分发征求意见的公约草案——暂名《非洲联盟建立适用于网络安全的法律框架公约草案》——可能在今年 1 月的亚的斯亚贝巴 AU 峰会上通过。公约宣称的目标是“通过组织电子交易、保护个人数据、推进网络安全、发展电子政务和打击网络犯罪，制订一个可靠的非洲网络安全框架”。在“权益和挑战”方面，《公约》旨在保护个人、组织和国家的数字与文化遗产；维护国家的生存和主权；保持一定程度的技术安全以阻止或控制技术与信息风险；建设一个尊重价值，维护权利与自由，保护个人、组织与国家财产安全的信息社会；推动知识经济，保障平等获取信息，鼓励创造真正的知识。[57]

由于技术滞后并出于对隐私与言论自由保护、立法过度以及法官权力过大等的担忧，《公约》目前已经推迟实施；[58]但预计会在 2014

和整体发展之间的关系。见“美洲国家组织：背景与国会议题”，彼得·梅耶（Peter J Meyer），2014，国会研究局，7-5700。

[56] 同上。

[57]《非洲联盟建立适用于网络安全的法律框架公约草案》，2012 年 9 月 1 日，http://au.int/en/sites/default/files/AU%20Convention%20EN.%20(3-9-2012)%20clean_0.pdf。

[58] 加瑞斯·范·齐尔（Gareth van Zyl）：“有瑕疵的非洲联盟公约推迟实施”，2014 年 1 月 21 日；“肯尼亚力图阻止有瑕疵的非盟网络安全公约实施”，2013 年 10 月 28 日，www.itwebafrica.com。

年 7 月或 2015 年 1 月通过。此外，在更广泛的国际网络安全事务中，非洲的参与度有限，如新一届 GGE 只有两个非洲国家。

见表 1：国际和地区安全（附件 1）。

3、国际和地区安全领域的双边努力

在双边层面，各国和其他利益攸关方间就国际和地区网络安全议题开展了多个 1 轨、1.5 轨和 2 轨对话。这些行动的主要目标是让参与各方更好相互理解，增加信任和信心，建立避免武装冲突的联合机制。1 轨对话的政策平台包括：中美在原有战略对话框架下的对话，还有中英、 中德和中欧对话；德国和美国，德国和印度；俄罗斯和印度，俄罗斯和巴西等。在这方面，美国跟日本、印度、巴西、俄罗斯、南非和韩国均有双边探讨。此外，东盟与日本、中国和美国还举办了相关的研讨会（见图 1）。

特别要指出的是，这些双边对话在 2013 年有所进展。2013 年 6 月，现有战略与经济对话框架下的中美讨论就系列措施达成一致，标志着双方向更大的合作迈出重要的第一步。双方同意建立一个工作组来“增进互信，减少互疑，应对分歧和扩大合作”。自 2013 年 6 月成立后工作组举行了两次会谈。[59]8 月，中国外交部长王毅对美国务卿约翰·克里表示，他视“网络空间”为“两国增进互信与合作的领域”，这是一项重大进展。此前，围绕美多次谴责中国网络工业间谍，以及美国会声称怀疑“中国电信公司对美电信市场进行持续渗透”，两国

[59] www.reuters.com/article/2013/11/06/net-us-usa-china-hacking-idUSBRE9A51AN20131106

间的紧张局势不断升级。[60] 中国官员也普遍认为美国公司是传递美国政治价值观的“特洛伊木马”。[61] 作为对斯诺登披露信息的回应，中国国防部发言人杨宇军表示，“棱镜门事件本身正如一面棱镜，折射出有关国家在网络安全方面的真实面目和虚伪言行。”[62] 毋庸讳言中国对美监视行动的关切也激起国内对中国政府自身监视行动的关注。[63]

2013 年，俄罗斯和美国也同意在“美俄双边总统委员会”（2009 年由美总统奥巴马和俄总统梅德韦杰夫建立）下新建一个工作组，负责“评估不断出现的 ICT 威胁并提出一些联合应对措施。”[64] 除组建工作组外，两国总统还参与对话以“增加透明度和减少对可能引发不稳定或危机的网络突发事件的误判”。[65] 该讨论最终形成由两国元首同意的三条建立信任措施。第一条是两国 CERTs 间建立联系，“促进就关键系统网络安全风险的技术信息进行定期交流”。第二条是通报措施，包括通过双方现有“核风险减缩中心”“快速、可靠的向对方主管部门提出要求，减少误判和 ICT 安全事件升级的可能性”。[66] 第三条是在白宫和克里姆林宫间建立热线电话，确保双方领导人“为应对其面临的所有国家安全危机做好准备”。[67] 但在工作组外双方关系恶化，美国

[60] http://intelligence.house.gov/sites/intelligence.house.gov/files/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf

[61] Geekwire,“中国对美国家安全局监控的反应引起微软公司的担忧”，2013 年 7 月 12 日。

[62]“中国国防部长指责美国在间谍问题的虚伪面目”,《纽约时报》，2013 年 6 月 27 日。

[63]“美国棱镜，遭遇中国金盾”,《纽约时报》博客，2013 年 6 月 28 日。

[64] http://www.whitehouse.gov/the-press-office/2013/11/22/joint-statement-inaugural-meeting-us-russia-bilateral-presidential-commi ，也可见: http://www.atlanticcouncil.org/blogs/natosource/us-and-russia-sign-cyber-security-pact 。值得一提的是，事实可追溯到 1998 年，美国和俄罗斯发表联合声明《21 世纪初面临的共同安全挑战》，其中特别关注“对于信息技术革命，趋利避害很重要（…），它是两国未来维护战略安全利益所面临的严峻挑战。”该声明为解决这些问题做了尝试。为解决 2000 年可能发生的“千年虫”问题，美俄成立防务咨询小组，双方在此框架下进行了“建设性讨论”。克鲁斯基赫（Krutskikh）等, 2009, (pp.148-149).

[65] http://www.state.gov/p/eur/cirs/usrussiabilat/c38418.htm

[66] 同上。

[67] http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information

国家安全局监控事实披露后，俄罗斯议会下院副议长谢尔盖·热列兹尼亚克呼吁俄“重申‘数字主权’”，通过立法要求所有俄用户的互联网通信数据应存储在俄境内服务器。[68] 俄罗斯在叙利亚冲突及近来乌克兰危机中的所作所为引发的战略关注，将在美俄关于信息通信技术应用双边讨论的走向上发挥显著影响。

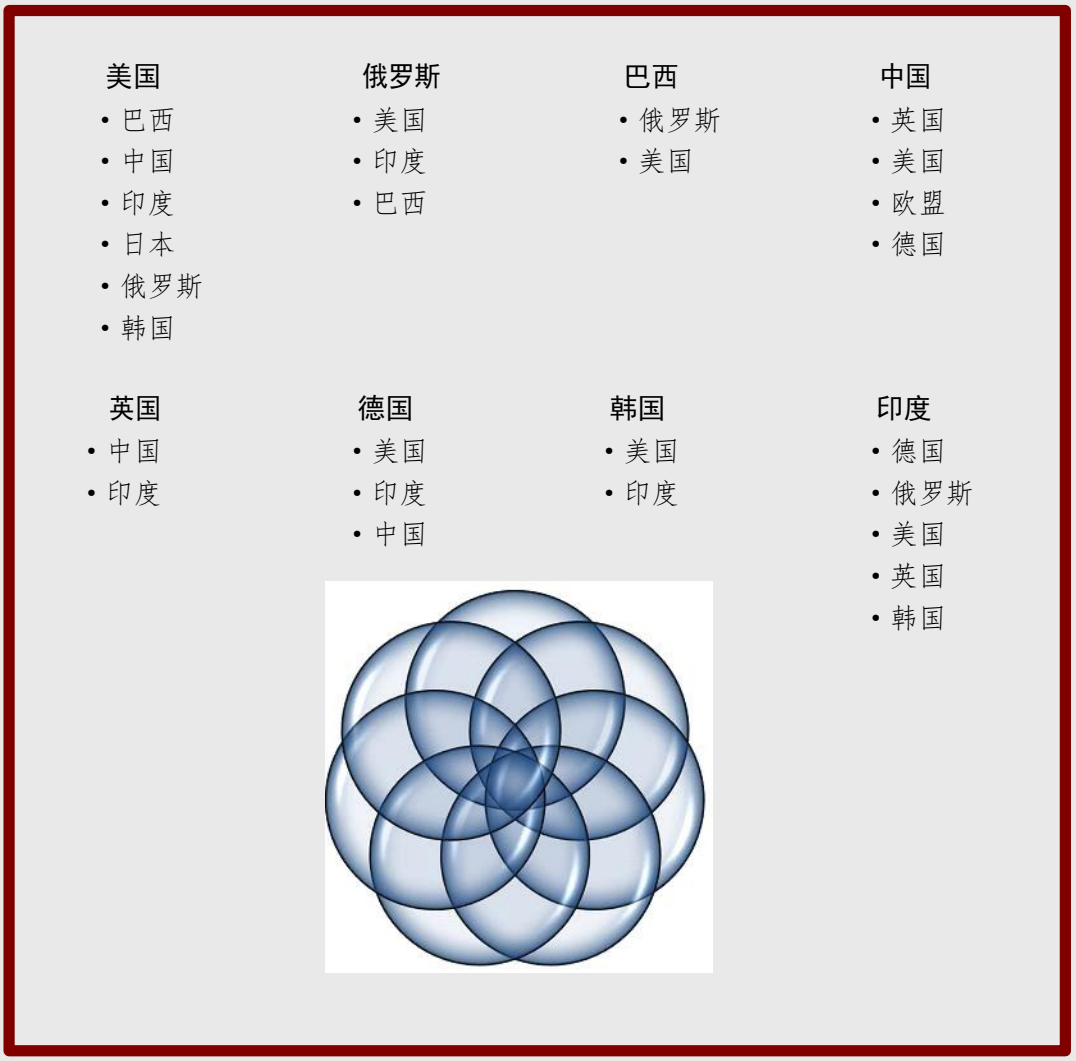

图 1：当前双边 ICT 相关进展的快照

[68] 安德烈·索尔达托夫（Andrei Soldatov）和伊莉娜·波罗干（Irina Borogan）：“俄罗斯是监控国家”，《世界政策杂志》，“秘密与安全”，2013 年秋季刊。

4、跨国犯罪与恐怖主义

4.1 网络犯罪国际公约？

过去十年，伴随互联网普及率的显著提高，个人和有组织犯罪团伙利用网络获取非法财富的网络犯罪活动不断增加。

联合国毒品与犯罪问题办公室(UNODC)近期研究表明，当今“高达80%的网络犯罪活动是有组织行为，已形成由恶意软件开发、计算机感染、僵尸网络控制、个人和财务数据盗取、财务信息出售等构成的网络犯罪黑市。”[69] 虽然受害率统计显示，相比传统犯罪，网络犯罪的受害者要多得多，但这些统计数据还不足以描绘出网络犯罪影响的准确图景。[70]

[69] 联合国毒品与犯罪问题办公室（UNODC）《网络犯罪综合研究（草案）》，2013 年 2 月，详见: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[70] 根据 UNODC 报告，当前警方记录的犯罪统计不能作为进行国际比较的可靠依据，尽管这些统计对于国家决策者具有重要参考意义。受害调查则能成为进行比较的更可靠依据。调查表明，网络犯罪的个体受害者数量远比“传统”犯罪形式的受害者多。全球 21 个国家的 1%到 17%的人口曾遭遇在线信用卡欺诈、身份窃取、网络钓鱼、未授权登陆电子邮箱等网络犯罪，而传统的盗窃、抢劫和偷盗机动车等犯罪率在相同国家均低于 5%。网络犯罪受害率在欠发展地区更高，凸显了强化保护措施的必要性。

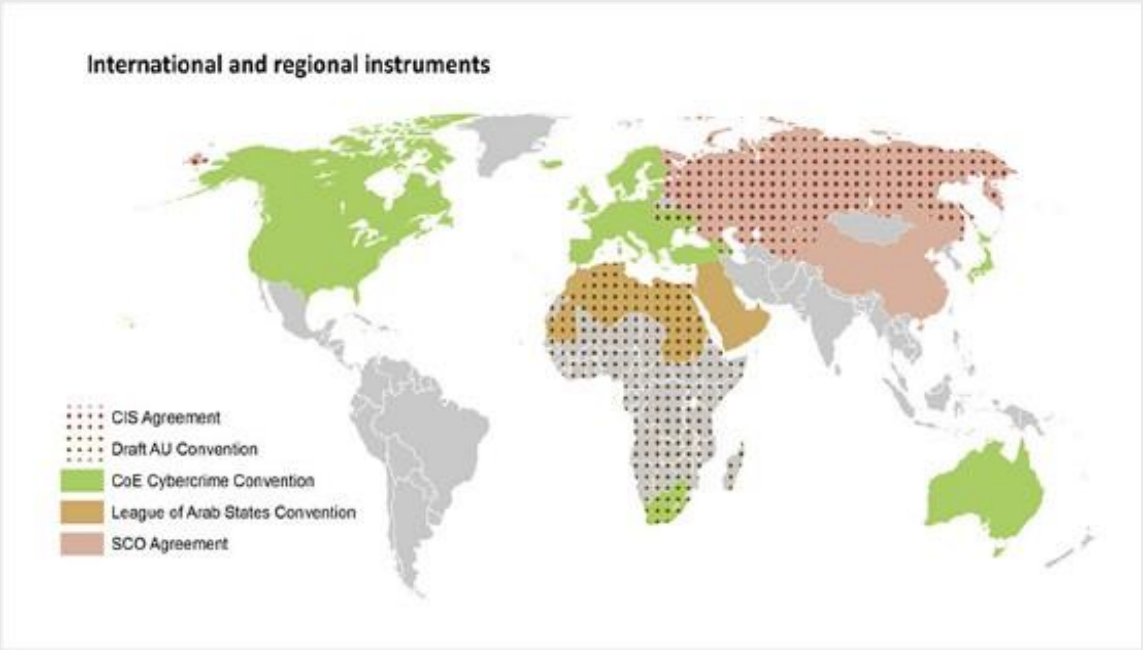

图 2. 来源： UNODC 网络犯罪综合研究，草案，2013 年 2 月

尽管一些国家的决策者和执法官员能够追踪犯罪分子并了解他们如何利用信息技术漏洞非法获利，但重大差距仍然存在。[71] 对发展中或“脆弱”国家而言，因执法能力弱，又有比花费高成本应对系统漏洞和追踪网络犯罪分子更为紧迫的任务，故此其面临的挑战更大。虽然越来越多的国家出台了网络犯罪法规，但仍有不少国家存在“司法空白”（jurisdictional voids），犯罪分子和入侵者难以受到惩罚。[72] 同时一些政府部门还可能越来越多地“默许建立信息安全港（与离岸避税港和银行保密一并）来招商，增加执法部门追踪信息和阻断非法网络商业活动的难度”。[73]

在之前关于建立一个应对跨国网络犯罪威胁的全球框架的讨论中，

[71] 参见例子，梅丽莎·哈萨维（2012）：“沦为网络犯罪牺牲品：对商业和经济的影响”，尼古拉斯·伯恩斯（Nicholas Burns)和乔纳森·普莱斯（Jonathon Price)主编：《保卫网络空间：国家安全的新领域》，阿斯彭研究所(2012 年 2 月)。
[72] 菲利·威廉斯（Phil Williams）：“有组织犯罪和网络犯罪：对商业的影响”，2005 年，参见：http://www.crime-research.org/library/Cybercrime.htm
[73] 同上。

主要关注是否按照美国和欧盟的提议，扩大 2001 欧洲委员会《网络犯罪公约》（即布达佩斯公约）的适用范围。[74]2012 年 7 月和 11 月，日本和澳大利亚的先后加入，使之朝着全球推广的方向迈出了一步。然而一些国家仍反对该公约，积极探讨在联合国框架下达成新的网络犯罪条约。这些迹象最早出现在 2008 年，2010 年在巴西召开的联合国预防犯罪和刑事司法大会上，与会方讨论如何应对公认的重大挑战时，此问题被明确提出。当时西班牙（时任欧盟主席国）建议任何有关网络犯罪的国际协议均应是布达佩斯公约的扩展，巴西予以反对并呼吁在联合国框架下制订新协定，以解决网络犯罪的地区性关切。[75] 俄罗斯也以“允许外国执法机构在俄罗斯境内进行互联网搜索违反其宪法”为由反对公约。[76]公约第 32 条有关“跨境进入经允许的或者公开存储的计算机数据”确实是最具争议的条款。[77]

是否起草一份新的国际网络犯罪条约仍是许多外交努力的重点，但新条约是否必要这一问题仍未解决，特别是考虑到不少地区性网络犯罪公约已经存在或正在起草。例如，之前提到的正处最后完成阶段的非洲联盟网络安全公约，重点解决网络犯罪问题。次撒哈拉非洲国家[78]网络犯罪活动不断增大的损失，“急需革新犯罪政策战略，从国家、

[74] 《网络犯罪公约》2004年生效。http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[75] 查尔斯·威尔德（Charles Wild），斯图尔特·威恩斯坦（Stuart Weinstein）， 尼尔·迈斯温（Neil Macewan），和尼尔·吉齐（Neal Geach）：《电子和移动商业法：数字时代贸易、金融、媒体和网络犯罪的分析》，哈福德郡大学出版社(2011)。

[76] 蒂姆·毛瑞尔 (2011)引用戈曼（Gorman）(2010)，“联合国制订网络规则：联合国网络安全活动分析”。哈佛大学肯尼迪学院，贝尔福科学与国际事务中心。

[77] 联合国毒品与犯罪问题办公室《网络犯罪综合研究（草案）》，2013 年 2 月，纽约。 参见：http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[78] 众所周知，喀麦隆、加纳、尼日利亚和南非已成为网络犯罪的集散地，特别是撒哈拉沙漠以南非洲地区的网络诈骗泛滥。例如，根据诺顿公司 2012 年的网络犯罪报告，南非的网络犯罪受害者数量位列世界第三。 另外，据南非网络犯罪威胁测量 2012/2013 估计，2011 年 1 月至 2012 年 8 月间，网络犯罪在南非造成的损失高达 26.5 亿。参见 www.itwebafrica.com。

社会和技术层面共同响应，为网络安全创建一个可信赖的法律环境”的强烈呼声，均激起当地国家起草公约的欲望。2012 年草案就准备完毕，随后在非洲次地区组织，如西非国家经济体（ECOWAS）和南部非洲发展共同体（SADC）举办了系列研讨会和咨询会。尽管草案受到隐私保护人士的批评，支持者则强调“此案力图解决一些在西方国家被利用的法律漏洞”。[79]草案预期在 2014 年 7 月或 2015 年 1 月正式完成并实施。

作为网络犯罪领域跨境合作法律与机制基础的其他区域性条约还包括 CIS 协定、阿拉伯国家联盟公约和 SCO 协定（参见图 2）。同时，一些国家团体（如金砖国家）的政治声明和宣言也包含重要的网络犯罪合作方面的内容。[80]

尽管如此，《布达佩斯公约》签约国继续主张扩大入约国家的数量，据称当前该公约仍是“制订网络犯罪立法最有用的多边机制”。[81]2013 年 11 月，欧洲委员会新发起为期三年的 GLACY 项目，目的是支持相关国家通过决策者参与协调立法、培训司法人员，强化执法能力，加强信息共享和国际合作以及评估进程等方式落实《布达佩斯公约》。[82]此前英联邦各国领导人也批准了一项倡议，推动成员国进一步向公约的基本原则靠拢。

尽管政治考量阻碍了就应对跨国网络犯罪最恰手段达成协议，但

[79] 详见博客文章：“非洲联盟网络犯罪公约”，参见：http://i.playgod.org/page/4/

[80] 详见《金砖国家决议草案：打击网络犯罪的国际合作》，呈交联合国预防犯罪和刑事司法委员会，维也纳，第 22 次会议，2013 年 4 月 22-26 日：临时议程第 7 条款——《预防犯罪与刑事司法领域的世界犯罪趋势和新兴问题》，联合国文件，2013 年 4 月 10 日。

[81] 同上。截至撰写本文时，《布达佩斯公约》签署国为 11，批准国为 42 个。参见 http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG

[82] 参见 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/GLACY/GLACY_en.asp

无论是传统的还是新型的打击犯罪国际合作措施,如引渡、司法互助条约（MLAT）、外国判决互认和非正式警方合作，或警方和相关技术公司的合作，都已在网络犯罪领域得以应用。事实上，正如 UNODC 提到的，传统形式的合作——特别是 MLAT——“在获取网络犯罪案件域外证据时优势突出”，大部分国家回归传统双边协议，只有少数国家使用多边协议。[83] 然而在证据搜集过程中，调查人员越来越多地获取境外数据（不管是公开的还是秘密的）“而未经数据所在国许可”的事实，有可能持续引发国家间的紧张。[84]

4.2 其他网络犯罪相关的措施、进程和发展

2010 年，联合国安理会主席声明首次正式确认网络犯罪和其他形式跨国有组织犯罪对国际安全的威胁。[85]正如第二部分提到的，2013 年 的UNGGE 框架，已就合作应对利用信息通信技术实施犯罪或恐怖活动达成一致（包括协调立法、执法和诉讼合作）。G8 等其他组织亦十分强调国际打击网络犯罪能力建设的重要性。

具体而言，联合国大会在 2010 年通过三个核心决议：2010 年 3 月通过的“创建全球网络安全文化”决议（A/RES/64/211）；2010 年 3 月通过的“授权加强联合国犯罪预防和刑事司法项目”决议（A/RES/64/179），特别强调网络犯罪领域的技术合作能力；2010 年 12 月通过的 A/RES/65/230 决议，召集网络犯罪国际应对的政府间专

[83] 联合国毒品与犯罪问题办公室调查报告指出，根据反馈，约60%的司法协助请求以双边机制为法律基础。采用多边机制的占 20%。

[84] 联合国毒品与犯罪问题办公室，《网络犯罪综合研究（草案）》，2013 年 2 月，纽约。 参见 http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[85] S/PRST/2010/4

家组并由 UNDOC 担任秘书处。2012 年，UNODC 建立政府专家组开展综合研究，目的是“促进对网络犯罪威胁的深入理解”并向“致力于应对网络犯罪、改进国家立法和能力建设的国家提供技术支持和培训”。[86] 研究提出六大问题：国际层面的碎片化、对传统正式国际合作措施的依赖、归因问题、国家法律框架的不一致、执法和司法能力的欠缺（特别是发展中国家）以及预防网络犯罪措施薄弱。[87] 这些研究借鉴了联合国预防犯罪和刑事司法项目及联合国犯罪委员会的相关工作。[89]2011 年，ECOSOC 犯罪委员会通过网络犯罪附加决议：“关于就经济欺诈和身份认证相关犯罪预防、调查、起诉和惩罚等开展国际合作”的 RES 2011/35 决议；以及“就利用新信息技术侵犯和（或）利用儿童开展预防、保护和国际合作”的 RES 2011/33 决议。

多年来，ITU 致力于在更广泛的网络安全战略框架下（即 ITU 全球网络安全日程，GSA），提升发展中国家应对网络犯罪的能力。其中部分工作关注在区域和次区域层次上协调国家立法和政策，包括与欧盟合作。2011 年，ITU 和 UNODC 签署谅解备忘录（MOU），在全球合作帮助成员国减少网络犯罪风险以及确保信息通信技术的安全使用。[90] 前文提到，自 2000 年初，OAS 开始着重强化本地区打击网络犯罪和利用信息通信技术实施犯罪的措施。如 20 世纪 90 年代以来，特别关

[86] A/RES/65/230

[87] 世界范围内，不到半数的被访者认为现有刑法和程序法足以应对网络空间的威胁。报告发现非洲联盟、独联体、欧洲议会、阿拉伯联盟和（或）上海合作组织的 87 个国家签署了打击网络犯罪的约束性文件。就定罪而言，报告指出14个国家中的13个普遍接受网络犯罪是犯罪，但大部分不认同传播垃圾邮件是犯罪。非法访问、非法截取、非法阻碍和计算机工具滥用则因网络特性而被认为是犯罪行为。至于警方和调查能力方面，“超过 90%的受访国已开始为网络犯罪调查和电子取证设置专门机构。”报告未指出在发展中国家的相关努力是否存在资源和能力不足的情况。国际合作方面，超过 79%的受访者开展了正式合作，其中的60%是以双边协议的形式达成，20%是多边协议。 联合国毒品与犯罪问题办公室,《网络犯罪综合研究（草案）》，2013年 2 月，纽约。

[89] 2010 年 3 月，A/RES/64/179

[90] http://www.itu.int/en/ITU-D/Cybersecurity/Pages/UNODC.aspx

注区域内毒品团伙如何利用信息通信技术和相关能力逃避执法、煽动恐怖和洗钱。如在墨西哥，Zeta 毒品团伙建立了从美国边境到危地马拉的独立通信网，[91] 逃避监控和执法部门的禁毒行动。2011 年末，墨西哥新拉雷多的一些博主惨遭毒品团伙虐杀，事后该团伙声称这些博主监控和参与有关墨西哥毒品现状的在线讨论并向有关部门告密。受害者被斩首或剖腹，暴徒还在其尸体上留言以警告类似在线活动。[92] 参与活动的美国学生也受到类似恐吓。[93] 墨西哥博主和记者担心这类攻击将阻碍人们使用互联网公布地方真相，在有组织犯罪已令传统媒体噤声之时，这种现象尤其让人担忧。[94] 墨西哥和地区当局努力加强合作以应对此类超越传统执法领域的威胁。

在跨境网络犯罪方面，OAS 的两个重要成果包括建立“美洲门户”和“网络犯罪工作组”。二者均为“加强（网络）犯罪调查和诉讼区域合作”美洲司法部长及首席检察官会议（REMJA）的成果。“美洲门户”旨在促进和整合 OAS 成员国政府专家在网络犯罪国际合作调查和起诉环节的协作和信息交换。工作组于 1999 年由 REMJA 建立，作为加强网络犯罪预防、调查和诉讼国际合作的主要地区论坛，鼓励成员国家间交换信息和分享经验；为强化 OAS 成员国间及与其他国际组织和机制的合作提供必要建议。[95]

OSCE 也将网络犯罪作为战略要务，支持在成员国成立政策机构

[91] 关于犯罪团伙如何利用信息技术手段规避执法请参见：卡罗米·卡瓦纳 (2013)，“变聪明并放大：应对发展中国家有组织犯罪”，纽约大学国际合作中心 (23-24 页)。
[92] “黑帮斩首博主传递消息”，《休斯顿纪事报》，2011 年 11 月 11 日。
[93] “蜘蛛和网：网络空间战争迷雾”，《经济学人》， 2011 年 11 月 24 日。参见：http://www.economist.com/node/21530146
[94] 同上。
[95] 美洲国家组织法律合作部: http://www.oas.org/juridico/english/cyber.htm

通过能力建设等措施应对网络犯罪威胁。[96]2012 年 1 月，OSCE 新建“跨国威胁部”，其中的“战略警务股”负责“增强执法能力以有效应对含网络犯罪在内的各种犯罪威胁”。[97]前文提及 2013 年关于建立信任措施的 PC.DEC/1106 决议，也涉及恐怖分子或犯罪分子使用 ICT 技术，尤其鼓励国家建立“现代化且有效的法律并在自愿的基础上加强双边合作，包括执法部门在内的机构间有效及时的信息交换以打击利用 ICT 的恐怖分子或犯罪分子”。[98]

在操作层面，2013 年欧洲委员会在位于海牙的欧洲刑警总部建立了欧洲网络犯罪中心。该中心作为欧盟对网络犯罪的响应中心，支持欧盟成员国“建设调查与分析能力及与国际伙伴开展合作”。[99]具体应对以下网络犯罪领域的问题：有组织团伙实施的、产生巨大犯罪收益的犯罪行为，如在线欺诈；对受害者造成严重损害的犯罪行为，如在线儿童色情；影响欧盟关键基础设施和信息系统的犯罪行为。[100]

1997 年以来 G8“高技术犯罪小组”十分活跃，在新兴犯罪预警（包括网络、电子等相关犯罪）及建立基本行动原则和机制（计算机司法鉴定原则和 24/7 联络点）方面扮演重要角色。2013 年，G8 正式宣布加强和扩大罗马/里昂高技术犯罪分组（High Tech Crime Sub Group）及 24/7 网络的工作。[101]2014 年，国际刑警组织在新加坡建立

[96] 詹姆斯·库卡恩（James Cockayne）和卡米罗·卡瓦纳：“盲目飞行：响应国际威胁的政治使命”，主题文章，纽约大学国际合作中心，《特别政治使命年度评估》（2011）。参见: http://cic.nyu.edu/sites/default/files/political_missions_2011_thematic_kavanagh_cockayne.pdf

[97] 欧洲安全与合作组织。《2012 年年度报告：构建信任》(82-83 页)。

[98] 参见欧洲安全与合作组织 PC.DEC/1106“建立信任措施初始列表”第六段。参见: http://www.osce.org/pc/109168?download=true

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

[100] 同上。

[101] G8 外长声明， 参见: https://www.gov.uk/government/news/g8-foreign-ministers-meeting-statement

全球网络犯罪中心—“全球创新综合中心”(IGCI),将其打造成“鉴定犯罪、创新培训、行动协同、伙伴关系等前沿研究和促进机构”。[102]

其他技术支持和能力建设措施还包括微软的新网络犯罪中心（位于美国西雅图），其致力于促进该领域的公私合作。[103] 牛津大学全球网络安全能力中心（Global Cyber Security Capacity Centre），其于伦敦网络空间会议（Conference on Cyberspace）后建立，关注发展应对跨国犯罪和其他网络安全挑战的能力。世界银行也资助了韩国首尔建立的卓越中心（Centre of Excellence），支持本地区应对包括网络犯罪在内的一系列网络安全挑战。

4.3 打击恐怖主义利用信息通信技术（ICT）的国际努力

2001 年美国“911 事件”以来，随着全球互联互通的增强和各语种社交网站的兴起，恐怖组织对网络的利用更为老练。“911 事件”后，极端组织被迫转入地下，把互联网作为沟通和扩大影响的完美渠道，把互联网作为筹集活动资金的重要手段 [104]。联合国的一项研究显示，1998 到 2006 年间，基地组织网站数量从 12 个增加到约 2600 个。[105] 同一研究也指出其他组织如伊拉克基地组织、克什米尔虔诚军，车臣圣战者、巴勒斯坦极端组织等都利用互联网开展活动。[106]

[102] http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation
[103] http://www.microsoft.com/government/ww/safety-defense/initiatives/Pages/cybercrime-center.aspx
[104] 联合国利用互联网进行恐怖活动工作组报告（2009）。参见：
http://www.un.org/en/terrorism/ctitf/pdfs/wg6-internet_rev1.pdf。
UNODC 在 2012 年发布的后续报告，参见：
http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
[105] 依照 1617 决议完成的《基地组织监视工作组第四份报告》（2005），参见：
https://www.un.org/sc/committees/1267/monitoringteam.shtml。另请参见迈克·雅格布森（Michael Jacobson）(2010),“恐怖分子融资与互联网”,《冲突与恐怖主义研究》2010 年第 4 期 33 卷。
[106] 同上。

2006 年，联合国各成员号称“协调国际及地区层面的努力，打击所有形式的网络恐怖主义活动”，并“将互联网作为防止恐怖主义扩散的工具，同时考虑到国家在这方面需要协助”。[107] 然而，正如 2009 年联合国反恐任务组（UNCTTF）《打击利用互联网进行恐怖活动》报告所言，没有一个统一的措施能解决此问题。[108] 报告并未关注“网络恐怖主义”，而是认为“在该领域面临的恐怖威胁并不明显，在联合国反恐框架下采取行动的必要性故不突出”。但报告亦指出一旦未来恐怖分子得以发动网络袭击并带来具体的威胁，“建立一个新的国际反恐机制以应对针对重要基础设施的恐怖袭击，可能是一个更合适和更长期的解决方案。”如果情况确实如此，需要更新关键基础设施的定义（通过协议到条约等方式），把信息基础设施纳入其中。[109]

这个问题在联合国决议和国际政策议程中也非常引人注目，尤其考虑到“在全球化社会中，恐怖分子越来越多利用信息通信技术、特别是互联网实施恐怖活动，如招募、煽动、募集资金、训练及策划等”。[110]

2012 年，UNODC 与 UNCTTF 合作发布了《利用互联网开展恐怖活动》报告，着重指出成员国在应对恐怖分子利用互联网时所面临的立法和诉讼等核心挑战。作为刑事司法实践的资源和能力建设工具，该报告还强调有必要“加强司法系统与私营部门间的合作以及国际合

[107] 《全球反恐战略》（2006）。参见: http://www.un.org/en/sc/ctc/action.html
[108] UNCTITF (2009)， 《打击利用互联网开展恐怖活动》，纽约，参见：http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_internet_wg_2009_report.pdf
[109] 蒂姆·毛瑞尔：“联合国制定网络规范——对联合国网络安全行动的分析” 讨论稿 2011-11，哈佛大学肯尼迪学院科技与公共政策项目，2011 年 9 月。
[110] 参见 2014 年 2 月 11 日通过的 A/RES/68/187 及之前所有涉及反恐的技术协助国际条约和决议。详见 http://www.un.org/en/terrorism/resolutions.shtml

作，尤其当相关数据的存储与留存分属不同司法管辖时”。[111] UNODC 的研究和随之而来的批评也成为安全政策和推进开放自由之间水火难容的例证。[112] 同时，另外几个 ICT 和恐怖主义相关问题，如利用审查制度打击网上极端主义等仍存争议。

参见表 2：跨国犯罪&恐怖主义（附录 1）

5. 治理，发展和人权

5．1 治理

互联网治理已成为一个越来越有争议的政策议题。正如下面将要讨论的，前几年这个话题主要是由信息社会世界峰会及其后续议程以及工作组主导。然而近来，由于一些国家已将互联网治理议题及其机制视为其国家安全利益的核心，它已越来越难以从更广泛的国际和地区安全相关政策进程中分离出来。同时互联网治理也和关于发展与人权的讨论紧密相关。

这场讨论中主要有两种完全不同的观点（这种简单二分有过分简化之虞）。一种观点是按照传统习惯将互联网视为“全球公域”，[113] 认为互联网治理与常说的自下而上及多利益相关方（包括政府、私营部门与公民社会等各主体参与）关系密切，它强调开放贸易，民主治理和尊重人权，尤其是信息自由流动与自由接入等原则。持这种观点的

[111] UNODC and UNCTITF (2012)，《利用互联网开展恐怖活动》报告，纽约，2012。参见：http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

[112] 加拉赫·瑞恩（Gallagher, Ryan）(2012)：“联合国报告透露在线追踪的国际协议”参见：http://www.slate.com/blogs/future_tense/2012/12/04/u_n_office_on_drugs_and_crime_report_reveals_international_protocol_for.html

[113] 美国国务卿希拉里·克林顿关于互联网自由的演讲，2011 年 11 月，见 http://secretaryclinton.wordpress.com/2011/02/15/secretary-of-state-hillary-clintons-speech-on-internet-freedom/

国家往往有着深厚的民主政治历史或对自由民主政治体系的渴望，它也得到公民社会和私营部门的支持。

持不同观点的其他一些国家倾向自上而下和从领土管辖的角度来治理网络空间。它强调国家主权和不干涉原则。一些国家将信息的自由流动和言论自由，尤其是通过网上社交媒体，视为国家权力的潜在威胁。它们认为互联网应通过国家规定和政策进行治理，即使技术问题也应由国家资助的技术机构来完成。这些国家对现行的多利益相关方模式极度不信任，一方面因为在他们看来担负互联网治理核心功能的机构，如互联网名称与数字地址分配机构（ICANN）和互联网号码分配机构（IANA）[114] 由美国政府通过商务部实施间接掌控；另一方面他们认为总体上美国企业在互联网所带来的经济增长中获利最大。

最近，一些国家认为，ITU 作为联合国下设的一个特别机构更合适承担互联网治理职能。专制政府一般持这种看法，因为他们担心 ICT 潜在的政治力量和破坏性影响。出于多种原因，包括不可忽视的经济考虑，他们还倾向于将互联网治理与国家和国际安全与经济发展相联系，将其与信息安全和信息环境等议题结合在一起。[115] 随着互联网及 ICT 对全球经济的重要性日益突出，战略价值突显，把互联网治理置于国际机构保护之下的问题也日益受到重视。

2012 年，ITU 召开世界电信大会，重新讨论 1988 年的“国际电信规则”。[116] 随着对互联网治理未来关注的增加，[117] 大会受到公私部门和互

[114] 关于 ICANN 和 IANA 的授权，见 https://www.icann.org/en/about/welcome；见 https://www.iana.org/about
[115] 参阅吉尔斯（Giles）和哈格斯泰（Hagestad） (2013)。
[116] 1980 年签署的国际电信条约 (ITRs)是一项旧条约，此后经历多次谈判。最近的一次谈判是在 1988 年，通过为国际电信交换提供更多便利来帮助全球的互联互通。来源：互联网协会。
[117] 例见罗伯特·麦克道威尔（Robert McDowell）：“联合国威胁互联网自由”，《华尔街日报》，2012 年 2 月

联网权力行动家们的高度关注。会议结果表明：“国际社会内部深度分化，互联网治理面临重大挑战”。[118]ITU 大会通常采取一致同意和不投票的做法，但此次大会却出乎意料，ITU 主席在最后阶段要求政府对修改后的、涉及互联网的条约进行投票。

会议记录显示 89 个国家支持新版条约，50 个国家表示反对。[119]反对者中包括美国，大部分欧洲国家以及一些非洲和拉美国家。这些分歧并没有得到调和，两种立场间的紧张气氛今后一段时间内将只增不减。 2012 年的 ITU 大会可谓是自 2003 和 2005 两届 WSIS 进程[120]（该进程奠定了当前多利益相关方模式的基础[121]）以来首次就互联网治理问题展开的政治斗争。

此外还有许多国家被称为“摇摆国家”，[122]对双方观点没有坚定立场。如印度，2011 年 10 月向联大提交了一份提议，要求建立一个“联合国互联网政策委员会”（CIRP）。[123]该提议以原来信息社会世界

21 日，见 http://online.wsj.com/article/SB10001424052970204792404577229074023195322.html?

[118] 2011 年末开始出现关于 2005 年 WSIS 进程以来 WCIT 可能成为互联网治理最具争议性的平台的报道。

[119] 见 http://www.techdirt.com/articles/20121214/14133321389/who-signed-itu-wcit-treaty-who-didnt.shtml

[120] 关于 WSIS 进程的详细信息，见“互联网治理进程：赛场观察”，来自 Access 的德伯拉·布朗（Deborah Brown）、来自 Global Partners Digital 的李·卡斯帕（Lea Kaspar）和乔安娜·瓦龙（Joana Varon），来自基金会技术与社会中心的盖图略·维加斯（Getulio Vargas），
http://wilkins.law.harvard.edu/events/luncheons/2014-02-04_veni/GPD_A3%20Map%20Flyer_P6_Reprint_Web%20version.pdf

[121] 米尔顿·穆勒（Milton Mueller）认为，虽然许多人认为 WSIS 正式将互联网治理多利益相关方模式合法化（通过 2003 年和 2005 年的相关文件），但事实上政府通过“对每个主体的不同职责进行分配，并使其权力最大化，即有权制定与互联网相关的公共政策，破坏了这一模式。”简言之，他认为“WSIS 的重要文件旨在确立国家主体在全球互联网政策制定中的重要作用，排除其他主体在政策制定中发挥直接作用”。见米尔顿·穆勒的博客，“重划职责：论巴西议程”，2013 年 12 月 18 日，见 http://www.internetgovernance.org/2013/12/18/revisiting-roles-on-the-agenda-for-brazil/ An essay by Ambassador。俄罗斯安德烈·克鲁斯基赫大使在一本有关信息安全的书中写道，俄罗斯的核心目标是兑现 “WSIS 进程中承认政府主导作用的条款”和“对信息社会发展中国际法、国内法及主权重要性的肯定”。克鲁斯基赫(2009)：“俄罗斯确保和平的信息外交的倡议（10 年历史）”，《国际信息安全：和平外交》，克鲁斯基赫编，2009 年，莫斯科。此外，穆勒尔（Mueller）指出，WSIS 的成果“如其所称的‘加强合作’和 成立 IGF 论坛，似乎要解决互联网治理的分歧”，但正如他所言，随后发生的各种事件表明并未达成一致。参阅米尔顿·穆勒尔（Milton Mueller）的博客：“透视巴西大会”，2014 年 1 月 14 日，见：
http://www.internetgovernance.org/2014/01/14/the-brazil-meeting-x-rayed/

[122] 例见埃伯特·汉恩斯（Ebert Hannes）和蒂姆·毛瑞尔 (2013)：“竞争的网络空间与崛起的力量”，《第三世界季刊》Vol. 34 Iss.6。

[123] 全文见：

峰会《日内瓦原则宣言》和《突尼斯议程》（建立了互联网治理论坛和“加强了合作的进程”[124]）的原则为基础。[125] 其中“加强合作的进程”已产生系列联合国决议、大会报告和咨询意见，以至 2012 年联大关于“用于发展的信息和通讯技术”决议（A/RES/67/195），开启了 2015UNGA 对 WSIS 突尼斯阶段成果文件进行评估的准备工作。[126] 决议邀请科学和发展委员会（CSID）主席建立一个工作组“以寻找，汇编和回顾所有成员国和所有其他主体提交意见的方式，评估 WSIS 授权的国际合作工作的进展，并对如何全面落实这一授权提供建议。”[128] 2014 年工作组将在 CSTD 第一次会上提交一份报告，全面回顾 WSIS 进程。[129] 2011 年在南非德班召开的印度、巴西和南非（IBSA）全球互联网利益相关方会议上也进行了类似的讨论。[130]

2013 年，联大再次通过决议（A/68/198），提出“根据《突尼斯议程》的第 111 段，尽快（不晚于 2014 年 3 月底）完成联大对 WSIS 成果的总体回顾。”决议还邀请“联大秘书长任命两名协调人公开征询各国政府的意见。”有趣的是，早期一个对 WSIS 评估的决议（A/C/C.2/68/L.40）肯定了 ITU 及其对 WSIS 的贡献，并邀请它继续

http://ibnlive.in.com/news/full-text-indias-united-nations-proposal-to-control-the-internet/259971-53.html

[124] 关于 WSIS 的背景信息见米尔顿·穆勒，《规范根本：互联网治理与网络空间规制》（2004），MIT 出版社；《网络与国家：互联网治理的全球政治》(2013)，MIT 出版社。亦见沃夫岗·克莱恩沃彻）（Wolfgang Kleinwächter）和丹尼尔·斯道法赫（Daniel Stauffacher）：“信息社会世界峰会：从过去到未来”(2005)，联合国工作组系列，见：http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=169379&lng=en

[125] 关于“加强合作”的源起（与互联网治理问题相关），据称是依据“WSIS 在涉及美国对负责互联网核心基础架构资源管理机构拥有监管权的谈判中，讨论了如何扩大其他国家的参与”，关于这一问题在突尼斯会议中未达成任何协议，故任命一名联合国秘书长互联网治理问题特别顾问，就 2006 年“加强合作”开展系列咨询工作。最新的“加强合作”进展包括联合国 2013 年 2 月 5 日通过的一项决议（A / RES / 67 / 195）。关于“加强合作”的详细信息见：http://linguasynaptica.com/timelines/enhanced-cooperation/

[126] 联大决议 A/RES/68/198 号决议中最后确认对 WSIS 的评估。

[128] 联大 A/Res/67/195 决议，《用于发展的信息与通讯技术》，2013 年 2 月 5 日。

[129] 同上。

[130] 埃伯特·汉恩斯（Ebert Hannes）和蒂姆·毛瑞尔 (2013)：“竞争的网络空间与崛起的力量”。

参与“峰会总体评估和准备工作”。但最后的决议撤掉了上述内容，这也许能表明相关国家背后在利用 ITU 问题上的紧张斗争。2014 年 10 月-11 月的 ITU 全权大会、新主席选举及 WSIS 评估将推进互联网治理相关讨论。

如上文所述，美国和英国的监控事件在政策圈，包括互联网治理圈引起掀然大波。巴西和德国联合起来在联大三委通过《数字时代隐私权》[131]的决议。接着，巴西宣布将于 2014 年 4 月召开一个全球峰会——“互联网治理未来之全球多利益相关方大会”。美国大使丹尼尔·塞普维德（Daniel A. Sepulveda）在 2014 年 1 月[132]发表演讲，在对这项措施的欢迎的同时，提出今年在伊斯坦布尔举行的 IGF 可能才是以“最具全球性和包容性”[133]方式解决上述问题的合适渠道。在向 ICANN 于 2013 年成立的“全球互联网合作与治理机制高级会议”上的发言中，他也建议研究互联网治理的未来。[134] 该小组的任期从 2013 年 12 月到 2014 年 12 月，据称将吸收巴西大会和将于 2014 年 4 月在爱沙尼亚召开的“自由线上联盟”（更多内容见下文）的成果。[135]

另外一个对当前互联网治理大势的回应是“互联网治理未来之蒙得维的亚声明”，该声明于 2013 年 10 月在乌拉圭蒙得维的亚由“负

[131] 联大决议：《数字时代的隐私权》，A/68/167，2013 年 12 月 18 日。见：http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167&referer=http://www.un.org/depts/dhl/resguide/r68_en.shtml&Lang=E

[132] 美国助理国务卿、国际通讯与信息政策协调官丹尼尔·塞普维达（Daniel A. Sepulveda）大使讲话，“地缘政治和互联网治理未来”研讨会，美国国际与战略研究中心（CSIS），华盛顿，2014 年 1 月 23 日，见：http://translations.state.gov/st/english/texttrans/2014/01/20140125291640.html#axzz2rWOH3Pso

[133] 同上。

[134] 高级别小组，见：http://www.icann.org/en/about/planning/strategic-engagement/cooperation-governance-mechanisms。亦见 IGP 博客：对高级别小组与互联网治理未来之巴西大会的分析，http://www.internetgovernance.org/2013/11/19/booting-up-brazil/

[135] “自由线上联盟”大会，塔林，2014 年 4 月，http://www.freedomonline.ee/sites/www.freedomonline.ee/files/docs/FOC%20Tallinn%20concept%20paper%20-%20designed%20ver2_0.pdf

责协调全球互联网技术基础设施的机构领导人”共同发起。[136]其重要性在于“它表达出对近来大规模监控事件破坏全球网络用户对互联网信任与信心的强烈关切”。[137]声明还明确需要“持续努力应对互联网治理挑战，集合所有力量解决全球互联网多利益相关方合作的问题。”此外，这些领导者们还呼吁“加快 ICANN 与 IANA 功能的全球化进程，营造一个所有主体、包括所有政府主体都能平等参与的治理环境。”[138]随后，2013 年 11 月 ICANN 建立了一个“全球互联网合作小组”，成员来自政府、公民社会、私营部门、技术团体和国际组织，该小组于 2013 年 12 月在伦敦举行了首次会议。同时，2014 年 3 月国家电信和信息管理局（NTIA）——一个专门负责向总统提供电信与信息政策咨询、在 ICANN 政府咨询委员会（GAC）代表美国政府的部门——宣布有意将关键互联网域名职能移交给一个全球多利益相关体。[139]作为第一步，NTIA 要求 ICANN 与全球各相关方提出一个将由其负责的互联网域名系统的协调功能移交出去的方案[140]。

2014 和 2015 年是理解互联网治理各相关进程实际进展的关键。虽然美国及持相同观点的国家致力于使互联网不受国家政府的控制，但一些人认为他们实际上“没有一个能够确保互联网安全与发展的统

[136] 见：“互联网治理未来之蒙得维的亚声明”，见：
http://www.icann.org/en/news/announcements/announcement-07oct13-en.htm

[137] 同上。

[138] 他们还呼吁：“将 IPV6 转型作为全球的优先考虑”，强调“互联网内容提供商尤其必须同时提供IPV4 和 IPV6 服务，以确保全球互联网的通畅”，见：
http://www.icann.org/en/news/announcements/announcement-07oct13-en.htm

[139] 2009 年 9 月 30 日，NTIA 代表美国商务部与 ICANN 达成协议，承诺将 DNS 的技术协调功能完全移交给一个由私营部门主导的多利益相关方，明确 ICANN 决策过程的问责机制和透明，保护全球互联网用户的利益，建立解决互联网 DNS 安全稳定和韧性的机制。http://www.ntia.doc.gov/category/icann

[140] 见 NTIA 新闻发布会：NTIA 有意移交关键互联网域名职能的声明，见：
http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

一战略表述，也没有提出一个足以对抗中俄等国模式的框架。”[141] 缺乏战略统一性在一定程度上与民主国家内部在“网络日程”上的相互竞争有关。另外，一些人还认为现有互联网架构和机制也许到了其生命周期的最后阶段，因为它们“不能有效应对互联网发展重心移向东半球和南半球的趋势；不能给新参与者在决策程序中提供应有的位置；无法应对高速增长的移动技术和云计算”。[142] 同样值得关注的是互联网治理与国际网络安全议题的持续融合，及此融合对两个领域内相关外交进程的影响。[143]

5．2 人权

保护人权，尤其是言论自由，已成为所有围绕网络空间展开讨论的重点。一个重要的里程碑就是 2012 年联合国人权理事会达成的决议“确保人们在网下的权利在网上同样受到保护”。[144] 一系列事件共同促成了这项决议的达成。如 2011 年 5 月，G8 发表了《重申对自由与民主的承诺》，[145]提到互联网提供了“独特的信息与教育资源”，宣言承认互联网作为提升人权、自由和民主的工具的巨大潜力，并强调开放、透明和自由是互联网成功与发展背后的核心趋动力。[146]

[141] 见：《网络规则工作会议预备报告》，罗杰·赫尔威兹（Roger Hurwitz），卡米罗·卡瓦纳，蒂姆·毛瑞尔和迈克·塞克莱斯特（Michael Sechrist）。该会议由加拿大多伦多大学全球安全研究中心、哈佛大学肯尼迪政府学院贝尔福科技与国际事务中心资助。项目名称为“国际网络关系探析”，由麻省理工学院、哈佛大学、微软及麻省理工计算机科学和人工智能实验室共同推进，见：
http://www.citizenlab.org/cybernorms/preliminary_report.pdf

[142] 同上。

[143] 来自蒂姆·毛瑞尔和麦瑞特·拜尔（Meritt Baer）即将出版的对震网病毒的研究。

[144] 联合国人权理事会，“人权理事会第 21 次会议报告”A/HRC/21/12，2013 年 8 月 26 日，见：
http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session21/A-HRC-21-2_en.pdf

[145] 达成的原则包括：“自由、尊重隐私和知识产权，多利益相关方治理，网络安全，预防危及互联网健康繁荣的犯罪”，G8 声明：《重申对自由民主的承诺》，G8 峰会，2011 年 5 月 26-27。对声明的批评可参阅第 19 条。

[146] http://www.nato.int/nato_static/assets/pdf/pdf_2011_05/20110926_110526-G8-Summit-Deauville.pdf

2011 年 9 月，欧洲委员会（CoE）发布了互联网治理原则、保护言论和集会结社自由等声明，涉及了互联网域名的管理，并向成员国提出了一系列保护和提升互联网全球性、统一性和开放性的建议。[147] 这些声明和建议明确了欧盟委员会推动互联网自由与开放的承诺，“所有成员国均应将此贯彻到制定国家与国际互联网政策中去。”[148] 关于互联网治理原则的声明还特别指出，互联网治理安排必须以“确保所有基本权利和自由得以保护，在不违背人权法的前提下确保各项措施的普遍、统一和相互关联。”[149] 上述原则构成了欧洲委员会 2012 年 3 月 15 日发表的《互联网治理战略（2012-2015）》的基础。

2011 年 10 月，英国外交大臣黑格在伦敦网络空间会议上提出了若干网络空间原则。[150] 这些原则旨在提供一个“推动国家、商业和组织间合作的基础”，并在随后的布达佩斯和首尔会议 [151] 中得以重申。它们与 OECD 和欧洲委员会提出的相类似，被建议作为“就网络空间行为努力达成更广泛协议的开端”。[152] 作为落实的第一步，2011 年 12 月 15 个持相同观点的国家共同签署了《海牙网络自由宣言》。[153] 海牙

[147] CoE 的原则关注：i)保护和尊重人权、民主和法治；ii) 确保多利益攸关方治理； iii)国家有责任制定尊 重互联网自由和个人权利的互联网相关公共政策；iv)互联网的全球性和全球接入的目标；vi)互联网的统一 性；vii)去中心化的管理；viii)开放的架构；ix）网络中立；x)文化与语言的多样性。见：https://wcd.coe.int/ViewDoc.jsp?id=1835773

[148] 同上。

[149] 同上。

[150] 黑格在其公开演讲中提到的七原则包括：政府在网络空间的行为需适度且要遵守国际法；每一个人需有能力接入网络，包括足够的技巧、科技，信心和机会；互联网用户需对语言、文化与思想的多样性予以足够的宽容和尊重；确保网络空间的开放以促进创新和信息、思想及言论的自由流动；需尊重个人隐私权和对知识产权提供应有的保护；所有主体需开展集体合作以应对犯罪分子网上活动带来的威胁；促进竞争的环境以确保对网络、服务和内容的投资获得公平回报。见：https://www.gov.uk/government/speeches/foreign-secretary-opens-the-london-conference-on-cyberspace

[151] https://www.gov.uk/government/speeches/foreign-secretary-opens-the-london-conference-on-cyberspace

[152] 同上。

[153] 声明签署国包括：奥地利、加拿大、捷克、法国、爱沙尼亚、加纳、爱尔兰、肯尼亚、马尔代夫、墨西哥、蒙古、荷兰、英国、美国和瑞典。承诺内容包括：建立信息分享联盟，包括网上损害言论自由和其他人权的行为的信息；通过政治协作和项目援助，实现个人权利（尤其在压制环境中）；与其他攸关方合作；双边和国际合作与民主；鼓励 ICT 企业反对可能危及互联网自由和个人权利的政策和行动。

会议以来，一些国家组建了“自由线上联盟”，成员涵盖 22 个分别来自亚洲，非洲，欧洲，美洲和中东的国家。[154] 接受《海牙宣言》的所有原则，尤其是所有人享有同网下一样的网上权利的核心原则是加入联盟的首要条件。[155] 该机构的主要活动包括通过外交协商提高互联网自由；支持公民社会；与私营部门合作鼓励公司采取尊重人权的行动与政策。与“自由网上联盟”并行的另一个非正式机制“数字保护伙伴”也在同期成立，标志着“一个前所未有的政府合作，得以为那些受到威胁的互联网用户提供紧急帮助，帮助他们通过新技术和平地履行普遍权利”。[156]

2011 年 12 月，34 个 OECD 国家连同埃及发布了《互联网政策制定的原则》[157]，所有参与方，包括政府，私营部门和公民社会同意遵循一些基本原则，承诺在制定互联网政策时要促进互联网的自由与开放。[158] 虽然 OECD 国家和埃及采用了相关建议，但公民社会代表还是于 2011 年 6 月底宣布，考虑到知识产权保护问题，他们不支持这个文件。[159]

总体上看，这些都是积极的进展。但如前所述，尽管上海合作组织（SCO）成员在他们通过提议的文件中（如行为准则）声称其原则与联合国人权宣言和其他人权条约一致，但他们始终坚持国家安全

[154] 参加国包括奥地利、加拿大、哥斯达黎加、捷克、爱沙尼亚、芬兰、法国、乔治亚共和国、德国、加纳、爱尔兰、肯尼亚、拉脱维亚、马尔代夫、墨西哥、摩尔多瓦、北爱尔兰、瑞典、突尼斯、英国和美国。

[155] 见“自由线上联盟”《简报》，美国国务院，2011 年 11 月 20 日，www.humanrights.gov

[156] 同上。

[157] OECD 原则包括：促进和保护信息的全球自由流动；促进互联网的开放、分布式和互联性；促进对高速网络和服务的投资与竞争；促进跨境服务；鼓励多主体合作参与决策；推动以自愿形式制订的行为准则；提升决策中使用公开和可信数据的能力；确保透明、公正和问责；强化在全球层面隐私保护的一贯性和有效性；个人赋权最大化；提高创造力和创新性；限制仲裁的责任；鼓励提升互联网安全的合作；给执法活动恰当的优先权。见: http://www.oecd.org/dataoecd/40/21/48289796.pd

[158] 同上。

[159] http://www.internetgovernance.org/2011/06/28/civil-society-defects-from-oecd-internet-policy-principles/

考虑必要时候高于人权关切。

前论指出，2013 年 NSA 和 GCHQ 网络监控行为的曝光，关于人权的讨论迎来了出人意料的转折点。一些国家已开始采取越来越严格的措施，常常利用法律与市场压力提升其要求网页和社交网络平台移除相关内容的正当性，并将监控责任转嫁给互联网服务商[160]（ISP）。许多民主国家采取“广泛监控措施对邮件、手机和其他通信行为进行监听，要求 ISP 保留相关信息并在必要时移交给执法部门。”[161]虽然这些问题前些年就引起关注，尤其成为联大关于“提升和保护言论自由”特别报告的焦点，[162]但 NSA 监控的曝光后各种政策反应才接踵而来。2013 年 10 月首尔会议上，瑞典外交部长卡尔·比尔特在演讲中提出指导国家监控行为的“七原则”；[163]2013 年 12 月联大第三委员会通过《数字时代的隐私权利》（RES/68/198）决议；联合国人权理事会发表《国家监控通讯行为对人权、隐私和言论自由的影响》报告。[164]

5．3 发展

在讨论安全、治理或人权问题时很难不涉及经济与社会发展问题，因为世界上的大部分人仍生活在贫困之中。[165]过去的二十年里，发展中国家不断强调弥合数字鸿沟的必要性，如“处于不同经济社会

[160] 罗纳德·戴伯特（Ronald Deibert），约翰·帕尔弗莱（John Palfry），拉法尔·罗霍兹恩斯基（Rafal Rohozinski）和乔纳森·兹特莱恩（Jonathan Zittrain）：《抗争的接入：亚洲网络空间的安全、认同与阻力》 麻省理工出版社，2012 年，第 31-32 页。亦见弗兰克·鲁（Frank La Rue）：“推动和保护思想与言论自由权利的特别年度报告”，A/ HRC/17/27 (Section 3) 。

[161] 罗纳德·戴伯特和拉法尔·罗霍兹恩斯基：“俄罗斯网络空间的控制与颠覆”，《受控制的接入：网络空间实力、权力与规则的塑造》，麻省理工出版社，2010 年，第 15-34 页。

[162] 报告列表，见：http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx

[163] http://www.regeringen.se/sb/d/17280/a/226590

[164] A/HRC/23/40 可在 http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/23/40&Lang=E 上查阅。

[165] 《2013 年人权发展报告》，
http://www.undp.org/content/undp/en/home/librarypage/hdr/human-development-report-2013/

发展水平的个人、家庭、企业和地域，无论是接入信息通信技术的机会，还是互联网的使用都存在很大差异。数字鸿沟反映出国内和国家间巨大的差异性”。[166] 其他诸如互联网连接和相关服务的质量，可负担性等也是需要重点考虑的问题。关于弥合数字鸿沟的讨论主要围绕下 列问题：经济的平等性，社会的流动性以及民主与经济增长。[167]2000 年的千年发展目标（MDGs）对 ICT 予以特别关注，MDG8 强调了建立“发展的全球伙伴关系”的重要性。更为具体的是，MDG 目标中有一项特别要求国家与私营部门合作“使新技术，尤其是信息通信技术的益处能被获取”。[168]

近来，上述讨论与其他涉及网络安全与网络犯罪的讨论交织在一起。中等收入国家，如巴西面临着重要挑战。巴西正着力解决国家低收入人群的宽带接入问题，但同时该国政府、商业及广大网络用户正遭受国内网络犯罪与网络攻击带来的巨大损失，其部分原因是平衡隐私和安全关切的关键立法迟迟未能出台。[169] 如果政府能够应对这些挑战，该国高素质技术人便能成为该领域能力建设的重要支撑。

西非，一个分布着 13 个最不发达（LDCs）国家的地区，16 个国家中的 14 个在世界发展排名中处在最低水平，[170] 该地区已成为世界

[166] OECD 统计术语表见：http://stats.oecd.org/glossary/detail.asp?ID=4719， 亦可参阅 OECD 出版物：《理解数字鸿沟》，http://www.oecd.org/internet/ieconomy/1888451.pdf

[167] 见《互联网世界国家：数字鸿沟、ICT 和 50x15 倡议》，见： http://www.internetworldstats.com/links10.htm

[168] 见 MDG 目标 8(f)，“千年发展目标和超越 2015”，见：http://www.un.org/millenniumgoals/pdf/Goal_8_fs.pdf

[169] 例见彭博通讯社，“为什么黑客涌入巴西”2013 年 9 月 13 日，见： http://www.bloomberg.com/news/2013-09-13/why-are-hackers-flooding-into-brazil-.html；《福布斯》,“黑客在巴西偷了 10 亿美元，使用云计算准备最差的国家”，2012 年 2 月 3 日，见：http://www.forbes.com/sites/ricardogeromel/2012/03/02/hackers-stole-1billion-in-brazil-the-worst-prepared-nation
-to-adopt-cloud-technology/

[170] 最不发达国家列表，参阅：http://www.nationsonline.org/oneworld/least_developed_countries.htm；《2013 年人权发展报告索引》，参阅：
http://www.undp.org/content/undp/en/home/librarypage/hdr/human-development-report-2013/

上最大的网络犯罪温床。[171] 当地执法部门在应对有组织犯罪和极端主义时也面临巨大挑战，因为后者能够通过尖端技术达到目的。[172] 但一直以来，发展机构不是很愿意将打击网络犯罪纳入其对发展中国家的援助之中，在某些场合宣称网络犯罪对穷人没有直接影响。[173] 但有迹象表明，这种看法已渐渐开始有所改变。

2000 年末以来，这些国家的能力建设日益得到重视，它们需要获得援助来“解决 ICT 的安全问题”，最新的 GGE 报告中有专门的部分来论述这一问题。更为具体地说，报告强调国家、尤其是发展中国家能力建设的重要性，并列出一系列能力建设的措施供国家参考。这些措施包括支持双边、区域、多边和国际能力建设的努力；加强国家法律框架、执法能力和战略；打击为犯罪和恐怖主义目的使用信通技术；协助确定和推广最佳做法；建立和加强应对事件的能力，包括计算机应急小组，并加强这些小组之间的合作；支持开发和利用关于信通技术安全的电子学习、培训和提高认识，帮助跨越数字鸿沟，并协助发展中国家了解最新的国际政策动态；日益增进合作并转让知识和技术，以管理信通技术安全事件；鼓励研究机构和大学进一步参与与信通技术安全有关的研究。[174]

GGE 报告还强调上述措施不仅有利于确保 ICT 的安全使用还能促进 MDG8 的实现。这种强调合乎时宜，MDG8 一度被视为 MDGs 中的“弱

[171] 科特迪瓦，加纳和尼日利亚在身份欺诈、信用卡盗取和各种形式的互联网犯罪方面声名远扬。
[172] 参阅卡瓦纳编(2013)，《变聪明和长本事：应对发展中国家有组织犯罪的影响》，纽约大学国际合作中心，可在 http://cic.nyu.edu/content/responding-impact-organized-crime-governance-developing-countries 查阅。
[173] 在伦敦进行的采访，2013 年 5 月。
[174] 同上，第五部分，关于能力建设的建议(第 30-33 段)。

项”之一，[175] 因为它主要从纯技术角度关注 ICT 的发展（如每百人中手机使用率和互联网接入率），在很大程度上与国际合作及社会经济现实相脱离。[176]

见附表 3：治理，发展和人权（附录 1）

6. 总结

过去十年里，各国对网络空间事务的兴趣与参与度均显著提升，因为它们越来越担忧国家和非国家主体对 ICT 恶意使用，并因之对国家、地区和国际安全造成的影响。那些国家利用 ICT 能力实施大规模网络监控的报道，使国家间信任与合作面临被严重破坏的风险；在控制网络时不能保障一些核心权利和遵守一些基本原则，也影响到国家和社会的关系。这种担忧正继续发酵，因此需要呼吁更多负责任的国家行为，呼吁在下列各领域达成协议：现有原则和规范的适用性；国家间透明度与建立信任措施；调整现有治理安排以及通过能力建设弥合发展中国家和发达国家间的数字鸿沟。各种国际和地区进程虽已取得一些重要成果，但仍需进一步将 2013 年达成的共识转化为具体可行的行动。合作与信任是当务之急，惟此才能应对现存的及正在生成的诸多压力，这些压力一方面作用于国际体系，另一方面也作用于发

[175] 联合国任务组关于 2015 年后联合国发展日程的报告，见：http://www.un.org/millenniumgoals/pdf/mdg_assessment_Aug.pdf

[176] 衡量是否达到 MDG 8 信息通信技术具体目标的核心指标包括： (i)每 100 名居民的固话普及率；(ii)每 100 名居民的移动电话数；(iii)每 100 名居民的互联网用户数。根据肯尼和戴斯翠的观点，除互联网用户和手机用户增加外，不能很好证明互联网和手机在促进经济和社会发展所有技术基础设施中发挥了极其重要的作用。见查尔斯·肯尼（Charles Kenny）和沙拉·戴斯翠（Sarah Dykstra） (2013)：“发展中的全球合作：对 MDG 8 的评估及对 2015 年后发展日程的建议”。该文作为背景研究文章提交给联合国发展日程高级别会议。亦见“联合国任务组关于 2015 年后联合国发展日程的报告”。

展中国家与发达国家的国家建设进程。

接下来的 18 个月对本报告所论各个进程的发展方向都十分关键。事实上，这些进程带给我们的更多是问题而非答案，如：

• 新一届联合国 GGE 会否就如何落实 2013 年国际规范和原则方面达成的协议？这一领域面临的主要障碍是什么？地区和双边进程会对 GGE 进程产生何种影响，反之如何？

• 如果国际体系在网络安全领域外面临严重的合法性危机，用什么能激励国家克制地使用 ICT 作为获得军事和政治影响的工具？联合国 GGE，OSCE 和 ARF 框架下达成的建立信任措施能否在国家间真正建立信任和透明？或者只是成为国家在无止境（且日趋危险）的战略博弈中提升能力的拖延手段？这种机制下恶意使用 ICT 并将其作为获取政治目标的手段会不会成为规范？

• 2013 年联合国 GGE 报告中有关鼓励公民社会，私营部门和学术界参与国际网络安全讨论的相关建议如何兑现？

• 国家间能否就应对网络犯罪和所有相关复杂的法律问题形成统一框架并达成协议？对国家主权问题的争论是否会成为永远阻止这种协议达成之障碍？如何才能避免这些结果的出现？地区层面能否有效保障打击网络犯罪合作的开展？从全球打击网络恐怖主义和反洗钱的国际合作机制和措施中能总结出什么经验？

• 决定互联网治理未来的不同进程将带来何种结果？这些大多由政府主导的会议得出的成果真有意义吗？会否滞后于市场趋和消费者选择的发展？在后续进程中如何继续把互联网治理与国际网络

安全议题整合在一起通盘考虑？

• 国际网络安全领域的能力建设能否对发展中国家实现 MG8 和 2015 之后的发展目标带来积极影响？如何衡量与评估这一进程？另外，提供能力建设援助者如何才能避免在传统安全和发展领域能力建设方面的陷阱？

• 最后，在所有这些进程中如何保护人权？

随着本报告中所列每一个进程的不断推进，上述及许多其他问题都值得认真思考。然而，达到这一目的需要各国更多的积极参与和负责任的行动。

附件 1

表

表 1 国际与地区安全

主要决议，声明，协议，决定与报告

2013	EU 网络安全 战略十 建议 x a 指令 (2 月)	G8 外长声明 (4 月)	UNGA A/68/98(1st COMM) 《从国际安全的角度来看信息 和电信领域的发展》，第二份GGE 报告 (6 月)	OSCE PARL. DEC.& RES. on CYB.SEC (7 月)
2012	OSCE PC DEC. 1039 《建立信任措施以降低使用ICT 带来冲突的风险》 (4 月)	OSCE MC DEC / 4 / 12 应对跨境威胁的努 力 （12 月）	AU AU / CITMC — 4 / MIN / Dect.(IV) 《对网络空间信息与安全条约 草案的背书一非最终稿》	UNGA A / 67 / 167 《从国际安全的角度来看信息和 电信领域的发展》，给秘书长的报告 （7 月）
2011	OSCE PC DEC.991 《OSCE 在网络空间的作用》 (3 月)	NATO 发表新的《网络防御政策》和行动计划 (6 月)	UNGA A / 66 / 152 及 A / 166 / 152 / Ad.1（一委） 《从国际安全的角度来看信息 和电信领域的发展》，给秘书长 的报告 （7 月）	UNGA A / 66 / 359（一委） 中国、俄罗斯、塔吉克斯坦、乌 兹别克斯坦给秘书长的信，《信息安全国际行为准则》 （9 月）
2010	AU ASS/AU/1 1(XIV) 《"非洲信息通信技术：挑战与发展前景"的声明》（落实2009 年关于制定网络安全 战略的决定） (2 月)	UNGA A / RES / 64 / 211 （二委） 《创建全球网络安全文化》 （3 月）	UNGA A / 65 / 154（一委） 《从国际安全的角度来看信息 和电信领域的发展》，给秘书长 的报告 （7 月）	UNGA A / 65 / 201（一委） 《从国际安全的角度来看信息和 电信领域的发展》，第一份 GGE 告报告 （7 月）
2009	SCO 《信息安全领域合作的协议》	AU 非盟部长会议要求非盟委员会准备非 盟网络安全条约 《Oliver Tambo 声明》	UNGA A / RES / 63 / 139 《从国际安全的角度来看信息 和电信领域的发展》 《第一委员会报告》(A / 63 / 385) （9 月）	UNGA A / 64 / 129 A / 64 / 129 / Ad.1 《从国际安全的角度来看信息和 电信领域的发展》，给秘书长的报告 （7 月 / 9 月）
2008	CSTO 《理事会有关成员国信息安全行动进展 的决议》 （9 月）	CIS 成员国首脑《有关信息安全领域合作的 决定》及行动计划 （10 月）	NATO 12 月峰会 第 47 条：实行网络防御政策 （12 月）	UNGA A / RES / 62 / 17 《从国际安全的角度来看信息和 电信领域的发展》 《第一委员会报告》(A / 62 / 386) （1 月）
2007	ITU 《全球网络安全议程》			
2006	UNGA A / 60 / 288 《联合国全球反恐战略》有关打击把互联 网用于恐怖目的的条款以及其他国际法律规定	UNGA A / 61 / 161（一委） 《 从国际安全的角 度来看信息和电信 领域的发展》 （7 月）	UNGA A / RES / 60 / 45 《从国际安全的角度来看信息 和电信领域的发展》 《第一委员会报告》(A / 60 / 452) （1 月）	WSIS 《突尼斯承诺》 WSIS—05 / TUNIS / DOC / 7—E（第 36 段，使用 ICT 推动和平与预防冲突） （11 月）
2004	OAS AG / RES.2004（XXXIV—0 / 04） 《美洲国家应对网络安全威胁的地区战略》	UNGA A / RES / 58 / 199 （二委） 创建全球网络安全文化等	UNGA A / RES / 59 / 61 《从国际安全的角度来看信息 和电信领域的发展》 《第一委员会报告》(A / 59 / 454) （12 月）	
2003	UNGA A / RES / 57 / 239（二委） 《创建全球网络安全文化》	UNGA A / RES / 53 《 从国际安全的角度来看信息和电信领域的发展》 《第一委员会报告》 (A / 53 / 505) （12 月）	WSIS 《日内瓦原则声明》 WSIS—03 / GENEVA / DOC / 4—E（第B5 段：在使用 ICT 中建立信任也安全） 《行动计划》 WSIS—03 / GENEVA / DOC / 5—E（第C5 段：在使用 ICT 中建立信任与安全）	
1998	UNGA A/RES/53/70（一委） 《从国际安全的角度来看信息和电信领域的发展》，是 1998 年 12 月 4 日 53/70 号决议、1999 年 12 月 1 日 54/49 号决议、2000 年 11 月 20 日 55/28 号决议、2001 年 11 月 29 日 56/19 号决议以及 2002 年 11 月 22 日 57/53 号决议的后续。			

表 1	国际与地区安全 主要决议，声明，协议，决定与报告			
2013	UNGA A / 68 / 156 及 A / 68 / 156 / Ad.1 《从国际安全的角度来看信息和电信领域的发展》及给秘书长的报告 （7 月 / 9 月）	UNGA A / RES / 68 / 243（一委） 《从国际安全的角度来看信息和电信领域的发展》（要求成立新 GGE） （12 月）	UNGA A / RES / 68 / 198（二委） WSIS 进展评估 （12 月）	OSCE 《使用 ICT 中建立信任以降低冲突风险的初步计 划》 （12 月） MS.DEC / 2 / 13 《加强打击跨境威胁的努力》 （12 月）
2012				
2011				
2010	NATO 爱沙尼亚政府有关网络防御的备忘录	AU AU / CITMC / MIN / DEC III ABUJA 声明（制订地区网络安全战略的确认决议）		
2009				
2008				
2007				
2006				
2004				
2003				
1998				

表 2 **跨境犯罪与恐怖主义**

有关决议，声明，协议，决定和报告

2013	EU 根据欧盟网络安全战略、建议及指令等在欧洲刑警组织建立网络犯罪中心 (2 月)	UNODC 对网络犯罪的全面研究 （2 月完成草案）	G8 外长声明 (4 月)	UNGA A/68/98(一委) 《从国际安全的角度来看信息和电信领域的发展》 第二份 GGE 报告（就国际法适用、网络空间的国家主权和国家责任等达成一致） (6 月)
2012	UNGA A / RES / 66 / 178 履行国际公约与协议、防止把互联网用于恐怖目的等 （3 月）	UNODA / UNCTTF 《把互联网用于恐怖主义目的的报告》		
2011	UN ECOSOC E / RES / 2011 / 35 《预防、调查、起诉和惩治经济欺诈及身份犯罪的国际合作》	UN ECOSOC E / RES / 2011 / 33 《打击使用新信息技术虐待和 / 或利用儿童方面的预防、保护及国际合作》	UNGA A.66.359（一委） 中国、俄罗斯、塔吉克斯坦、乌兹别克斯坦《信息安全国际行为准则》中有关网络犯罪的条款 （9 月）	
2010	UNSC 元首声明 S / PRST / 2010 / 4 《跨国威胁对国际和平与安全的威胁》 （2 月）	UNGA A / 64 / 211（二委） 《创建全球网络安全文化》 （3 月）	UNGA A / RES / 64 / 179（三委） 加强联合国打击犯罪及相关司法工作 （3 月）	UNGA A / RES / 65 / 230 《萨尔瓦多声明》 （12 月）
2009	SCO 信息安全领域合作的协议	G8 司法及内政事务部长的最后声明	AU 开始起草网络安全条约 （2013 年 1 月完成）	UNCTTF 有关打击把互联网用于恐怖主义目的的报告
2008	CSTO 理事会有关成员国加强信息安全合作的决议 （9 月）	CIS 元首决议，同意在信息安全方面进行合作及行动计划 （10 月）		
2004	CoE 《网络犯罪公约》	OAS AG / RES. 2004（XXXIV －0 / 04） 美洲内部打击网络安全威胁的地区战略	G8 高技术犯罪小组 《华盛顿公报》 （1997 年起开始采取行动）	

表 2 跨境犯罪与恐怖主义

有关决议，声明，协议，决定和报告

2013	UNECOSOC E / RES / 2013 / 39 《预防、调查、起诉和惩治经济欺诈及身份犯罪的国际合作》 （7 月）	OSCE PC DEC. 1106 《使用 ICT 中建立信任以降低冲突风险的初步计划》 （12 月）	OSCE MC.DEC/2/13 强化打击扩跨境威胁举措 （12 月）
2012			
2011			
2010			
2009			
2008			
2004			

表 3

互联网治理，人权与发展

有关决议，声明，协议，决定与报告

2013	UNGA A / RES / 67 / 195（二委及 ICT） 第二委员会报告 A / 67 / 3 / 434 （2 月）	UNGA A/68/65-E/2013/11 信息社会世界首脑会议成果在区域和国际两级落实和后续工作方面取得的进展秘书长的报告（3 月）	UNGA-ECOSOC/CSTD E/2013/31-E/CN. 16/2013/5 关于科学技术促进发展委员会第 15 次会议的报告（6 月）	UNGA A/Res/68/98(一委) 信息通讯领域在全球安全视野下的进展 GGE 报告第 2 号 （6 月）	网络空间首尔会议 一个开放安全的网络空间 （10 月）
2012	UNGA A/67/65/-E/2012/48 (二委及 ICT 进展) IGF 改进工作组的报告 （3 月）	UNGA A/67/66-E/2012/49 (二委-ICT 进展) 信息社会世界首脑会议成果在区域和国际两级落实和后续工作方面取得的进展秘书长的报告（3 月）	UNGA E/2012/31- E/CN. 16/2012/4(SUPP. 11) 关于科学技术促进发展委员会第 15 次会议的报告（5 月）	UNGA E/RES/2012/5 信息社会世界首脑会议成果落实和后续工作进展情况评估 （8 月）	联合国人权理事会 A/HRC/21/12 人权理事会 ITS 第 21 次会议的报告
2011	UNGA A/66/64-E/2011/77(二委及 ICT 进展) 信息社会世界首脑会议成果在区域和国际两级落实和后续工作方面取得的进展 秘书长的报告（3 月）	UNGA A/66/67-E/2011/79(二委及 ICT 进展) IGF 改进工作组的报告 （4 月）	UNGA A/66/77(二委及 ICT 进展)秘书长关于强化在与互联网有关的公共政策问题上的合作的报告（5 月）	G8 重申自由民主承诺的多维尔宣言（5 月）	OECD 互联网政策制订要点
2010	UNGA（CSTD） E/2010/31 E/CN. 16/2010/5 加强合作小组的报告（5 月）	UNGA E/RES/2010/2 信息社会世界首脑会议成果落实和后续工作进展情况评估(7 月)	IGF 维尔纽斯互联网治理论坛 （11 月）		
2009	UNGA A/RES/63/202(二委及 ICT 进展)第二委员会报告（A/63/411）联大 2008 年 1 月通过	UNGA (A/64/64-E/2009/10)(二委) 信息社会世界首脑会议成果在区域和国际两级落实和后续工作方面取得的进展秘书长的报告（3 月）	UNGA （E/2009/92*）(二委) 秘书长关于强化在与互联网有关的公共政策问题上的合作的报告 （7 月）	IGF 沙姆沙伊赫互联网治理论坛 （12 月）	
2008	UNGA （A/63/72-E/2008/48）(二委及 ICT 进展) 信息社会世界首脑会议成果在区域和国际两级落实和后续工作方面取得的进展 秘书长的报告（4 月）	UNGA （A/63/411）(二委及 ICT 进展) 2009 年联合国秘书长向经济及社会理事会提交“一份关于加强必要合作进程建议的报告”（12 月）	IGF 海德拉班德论坛 （12 月）		
2007	IGF 里约热内卢论坛				
2006	UNGA A/RES. 60/252 WSIS (4 月)	IGF 雅典论坛	联合国特别顾问就加强合作给秘书长的报告（4 月）		
2005	UNGA (第二委员会) A/RES/59/220 WSIS (2 月)	WSIS 突尼斯信息社会议程 WSIS-05/TUNIS/DOC/6-E (11 月)	WSIS 突尼斯承诺 WSIS-05/TUNIS/DOC/7-E (11 月)		
2003	UNGA (第二委员会) A/RES/57/238 WSIS	WSIS 日内瓦信息社会问题首脑会议 WSIS-03/GENEVA/DOC/4-E 行动计划 WSIS-03/ENEVA/DOC/5-E			
2002	UNGA (第二委员会) A/RES/56/183 WSIS				

表 3

互联网治理，人权与发展

有关决议，声明，协议，决定与报告

2013	网络空间首尔会议 指导国家监控的七条原则 （10 月）	IGF 巴厘会议 （10 月）	蒙得维的亚关于 IG 未来的宣言 （11 月）	UNGA A/RES/68/198（第二委员会） 用于发展的信息和传播技术 Dec. 2014 年 1 月通过	联合国人权理事会 A/HRC/23/40 关于国家监控对隐私和言论自由影响的特别报告	UNGA A/68/167 （第三委员会） 第三委员会报告（A/68/456/Add. 2） 数字时代的隐私权（12 月）		
2012	UNGA A/67/357 关于言论自由的特别报告 （9 月）	IGF 巴库会议 （11 月）	UNGA A/67/3\434 第二委员会报告 ICT 及发展 （12 月）	WCIT 迪拜最后决议 （12 月）		CoE CM（2011）175 final 网络治理战略		
2011	UNGA A/66/290 互联网言论自由报告 （8 月）	CoE 互联网治理原则宣言 （9 月）	CoE 关于保护言论和集会自由的宣言 （9 月）	IGF 内罗毕会议	网络空间伦敦会议 网络空间原则	印度 关于互联网相关政策向联大提交的建议 （10 月）	IBSA 茨瓦纳宣言（52-55） 与环球网络治理 IBSA 会议成果 （10 月）	关于网络自由的海牙宣言 （11 月）
2010								
2009								
2008								
2007								
2006								
2005								
2003								
2002								

关于信息通信技术和平基金会

信息通信技术和平基金会（网址 www.ict4peace.org），源于 2003 年日内瓦召开的联合国信息社会世界峰会（WSIS），旨在通过更好的理解和运用 ICT，促进政府、民众、社会团体和利益相关方开展有效和持续的沟通，更好地预防冲突、调解矛盾与维护和平。本基金会“网络空间的权利与安全”项目始于 2011 年。我们志在跟进、支持和领导双边及多边的外交、法律和政策行动，努力构建一个安全、繁荣和开放的网络空间。基金会的出版物可在 http://ict4peace.org/?p=1076 查找，主要包括：

- 着手实施：促进网络空间和平的现实目标（2011）
- ICT4Peace 关于即将在纽约召开的联合国网络安全政府专家组会议（GGE）的简报（2012）。
- 对全球和地区进展、议程和措施的概述（2013）
- 下一步干什么？网络空间信任措施建立（2013）
- 获取应对国际网络安全挑战的软实力（2013）