联合国网络规范的出现：

联合国网络安全活动分析

[美]蒂姆·毛瑞尔

曲甜、王艳译

资助致谢

本研究由海军研究办公室资助，授权编号：N000140910597。本文所有观点、研究发现、结论或者建议仅代表作者观点，不代表海军研究办公室观点。

摘要

网络战争不再仅存于科幻小说中。政策制定者就使用哪种规范来指导网络空间行为展开了全面的辩论。而联合国正是发生这场辩论的场所之一，也是本文关注的焦点。较之典型的国际关系时间轴，在过去的十年里，联合国在网络规范制定的工作中展现出了惊人的速度。最近，俄罗斯和中国（以及塔吉克斯坦和乌兹别克斯坦）于 2011 年 9 月一同提出了一项“信息安全行为国际准则”。2010 年，美国改变了其长期所持的政策立场，首次成为一项关于网络安全决议草案的共同提案国。这项决议草案早在 1998 年即由俄罗斯联邦向联合国大会提出。大体上说来，联合国网络安全谈判可以分为两个最主要的派别：一个是关注网络战争的政治-军事派别，另一个是关注网络犯罪的经济派别。我着重的是与以下情况有关的各种信号和趋势：管理网络空间的规范正在逐步形成，并向规范扩散发展。同时，我将证明这一过程是动态的。基于政治科学家玛莎·芬尼莫尔（Martha Finnemore）和凯瑟琳·斯金克（Kathryn Sikkink）提出的规范生命周期（norm life cycle）模型，本研究将探讨以下问题：联合国各会员国和联合国各机构等规范倡导者就网络安全做了哪些工作？为什么这些工作在不同时期有所变化？第一部分将提出关键的定义和概念。在第二部分，我将分析联合国中倡导规范的国家之间展开的辩论。这一历史分析分为两个方面：我将首先关注与网络战争相关的政治-军事派别，然后关注与网络犯罪相关的经济派别。第三部分将阐述互联网治理论坛（简称 IGF）的历史，以此丰富我的结论。

目录

导论[1]

2011 年 1 月 15 日，《纽约时报》报道，“震网病毒似乎是导致[伊朗]核问题耗时较长的重要因素之一，这也是迄今为止所部署过的最复杂的网络武器。”[2]2003 年之前，理查德·D. 克拉克（Richard D. Clarke）一直在白宫负责网络安全协调工作，就在几个月之前，他写道：“鉴于各方脆弱程度不一，有效限制国家在实际情况中运用其网络战争知识做的事情，或许是美国国家利益所在。”[3]这告诉我们三件事情。首先，这提醒我们网络战争不再仅存于科幻小说中。第二，美国和国际的政策制定者已就采取何种规范来引导网络空间行为展开了全面的辩论。第三，对国家利益的新定义将和如何利用新型潜在技术作战相互影响。

联合国是这场辩论的主要场所之一，也是本文所关注的焦点。有趣的是，一边是网络安全、震网病毒和维基解密一起占据了 2010 年的头版，另一边，在联合国一间小会议室里也发生了一些值得注意的事情：美国改变了其长久以来的政策立场，首次成为关于国际安全信息和电信技术的决议草案的共同提案国。“安全信息和电信技术”这一概念现在通常被简称为“网络安全”，是由俄罗斯联邦于 1998 年提出来的。[4]最新的进展是，俄罗斯政府和中国政府（以及塔吉克斯坦和乌兹别克斯坦政府）于 2011 年 9 月 14 日提出了“信息安全行为国际准则”，下一次联合国大会将对其进行讨论。[5]而仅在一周之后，俄罗斯就公布了一份关于“国际信息安全公约”的构想。[6]

2010 年 7 月，联合国一个由来自美国、俄罗斯和中国的外交官[7]组成的政府专家小组发表联合声明表示：“信息安全领域现存和潜在的威胁是二十一世纪最严峻的挑战之一”。2004 年建立的第一个专家组甚至无法达成最基本的共识，这使专家组秘书长于 2005 年不得不做出以下结论：“鉴于所涉问题的复杂性，未在编写最后报告时达成共识。”[8]

---

[1]我要感谢小约瑟夫·S. 奈很有帮助的评论和支持。特别感谢德国柏林的全球公共政策研究所，尤其是该所的副主任托尔斯滕·本纳（Thorsten Benner）。他给我提供机会让我在 2010 年夏季可以在该所担任访问研究员。全球公共政策研究所的工作人员为我提供了理想的、令人兴奋的环境。我尤为感谢奥利弗·里德（Oliver Read）帮助我编辑手稿。哈佛大学肯尼迪学院的文卡特斯赫（Venkatesh “Venky” Narayanamurti），以及迈克尔·西克里斯特（Michael Sechrist）的耐心支持，对于本文的成文至关重要。

[2] Broad et al, 2011

[3] Clarke and Knake, 2010: 226

[4]UN General Assembly A/RES/53/70

[5] UN General Assembly A/66/359;参见附录。

[6] Russian Federation 2011

[7] UN General Assembly A/65/201: 2

[8]UN General Assembly A/60/202: 2

联合国网络安全谈判可以分为两个主要的派别：一个是关注网络战争的政治-军事派别，另一个是关注网络犯罪的经济派别。两方均显示出管理网络空间的规范正在缓慢出现，并向规范化扩散发展。这些信号包括，联合国大会第一委员会的辩论已经持续十余年，十二个联合国部门中超过一半的部门已参与到过去五年这一最引人注目的问题中，以及关于行为准则的最新提案。然而，总体的趋势无法解释活动中的变化。比如，为什么在 1998 至 2004 年间一阵紧锣密鼓的活动之后，美国却在接下来的四年投票反对俄罗斯的决议草案？自布达佩斯《网络犯罪公约》于 2004 年生效之后，网络犯罪的谈判又有哪些进展？因此，我的研究将回答以下问题：作为规范倡导者的联合国会员国和联合国各部门究竟在网络安全方面做了哪些工作，以及为什么不同时期的工作有所变化？

美国的立场变化究竟是一种战略上的转变，从布什政府到奥巴马政府的战术变化，还是对俄罗斯采取的“重置策略（reset policy）”的回应？对此作出确切的回答为时尚早。然而，政策的变化和政府专家组的报告都可以作为政治信号。这些信号相当重要，因此我们应当更加仔细地分析联合国针对网络安全问题采取了哪些措施。比如，国际电信联盟（简称 ITU）秘书长表示支持网络和平行动。该行动是一次“通过改变立场以使网络战争非法化的尝试”，并在网络袭击、网络战争[9]和“电子珍珠港”[10]等话语主导的辩论中提供了一种反叙事（counter-narrative）视角。

在国际关系理论方面，我的研究发现与政治科学家玛莎·芬尼莫尔和凯瑟琳·斯金克提出的规范生命周期模型一致。因此，我采用她们的模型来指导我的分析。我的目标是首先阐释规范生命周期的开始阶段，也就是规范出现的阶段，然后阐释国际网络空间制度建立初期的状况。正如前文提及，联合国是这些辩论发生的最早期和最重要的场所之一。但该模型未能对网络规范形成过程中的各种起伏作出解释。

本文第一部分是理论部分，我将提出关键的定义和概念。接下来在第二部分，我从历史的角度，分析了联合国倡导网络安全的国家在这一问题上的辩论。这一分析强调了两方面内容。一是与网络战争有关的政治-军事派别，另一个是与网络犯罪相关的经济派别。我强调这一活动分为几个不同的阶段，并对以下两个问题作出解答。第一，美国与联合国的关系在 2005 年降至历史低点，这一状况如

[9] See Nye, 2011 3-4 for a brief discussion of the term“cyber-war”
[10] Wegener, 2011: 77; Schwartau 1991

何联系到2005至2008年的衰退？第二,政府更迭如何导致了2008至2010年的政策转变，并使网络争端占据头条？针对组织性平台，我提供了一幅联合国参与网络安全建设的各机构图解。我希望该图解能为未来更详细地分析每一个平台提供基础，但这超出了本文的范围。第三部分是关于IGF的，我描述了这一相对年轻的制度的历史，目的是使我之后的结论更加全面。

从方法论上讲，过程追溯是本文分析的核心方法。所有信息从主要文献和次要文献中收集，并由联合国官员访谈资料补充。我对他们所付出的时间和支持深表感谢。为了保护这些要求匿名的受访者，我在文中不具体指出他们的身份。另外，由于大多数联合国的部门只有为数不多的官员负责网络安全的工作，他们的身份非常容易被识别。然而，在大多数情况下，他们提供的信息都得到了二手公开资料的支持。若资料中无处可查，至少由出现在本文中的另外两处信息加以证实。

Ⅰ.理论基础、定义和概念

Ⅰ.1. 网络的定义与国际合作

“网络”一词在英文中作为前缀（Cyber-）指的是电子技术和以计算机为基础的技术。[11]网络空间（Cyber-space）是“一个由电子技术构成的操作领域……通过相互连接的系统及其相关的基础设施来利用信息。”[12]因此网络空间是“一种独特的混合制度，混合了物理特征与虚拟特征”，混合了硬件与软件，它与世界上包括互联网在内的所有计算机网络和其他网络都有所不同,而且并不连接到互联网上。[13]

互联网是网络空间中最大的网络，它被设计成“开放、极简和中立的”。[14]然而互联网的架构却要依情况而定，它是“一种选择——并非命运，并非注定，也并非自然法”。[15]在中国或者沙特阿拉伯可以找到例外的证明。“边界互联网”（bordered internet）的出现是通过各国互联网架构的变化完成的。这种变化受各国法律、技术发展以及更宏观层面的文化偏好影响。其中，技术发展使某些政策的实行成为可能。[16]

[11]关于国际关系研究和网络安全的概要，参见Eriksson et al; Nazli
[12]Kuehl cited in Nye, 2010: 3
[13] Nye, 2010: 3; Clarke and Knake, 2010: 70
[14] Wu and Goldsmith 2008: 23
[15] Wu and Goldsmith, 2008: 90
[16]Wu and Goldsmith, 2008: 149-150

然而，从技术角度看，互联网仍然是“无边界的”。在国际关系理论中，与“无边界的”对应的形容词是“跨国的”或者“全球的”。各国立法的确从法律上构建了边界，而且时常通过具体的技术特征来创造边界，比如中国的防火墙。虽然这一点确凿无疑，但是互联网最初的设计是无视国家边界的。互联网的设计中并没有政府的干涉，除非采取某些特殊的干预来改变这一属性，否则它就是没有边界的。

因此，用户可以在一个国家采取行动而在另一个国家产生结果，而该用户无须离开他的国家。这样的行动可能是善意的，也可能是恶意的，并且潜在地利用了各国司法和国际司法中的漏洞。事实上，ITU 的秘书长指出“根据某些统计，已经有超过六个国家在过去三年内遭受了网络攻击，并且至少有 34 个私人公司仅在 2010 年的头几个月就受到了袭击。”[17]

ITU 对网络安全作出了定义，即“工具、政策、安全概念、安全防护、指导原则、风险管理的方法、行动、训练、最优活动、保证和技术的集合。该集合可以用于保护网络环境、保护组织以及用户的资产。”[18]根据哈佛大学教授约瑟夫·奈（Joseph Nye）的研究，网络安全主要受到来自四个方面的威胁：间谍、犯罪、网络战争和网络恐怖主义。[19]潜在威胁的存在首先要追溯到三个源头，“(1) 互联网设计上的瑕疵；(2) 硬件和软件上的瑕疵；(3) 将越来越多的重要系统放在互联网上的趋势。”[20]

网络实力（Cyber-power）是指“‘在其他 30 个操作环境和广泛的权力工具中，运用网络空间创造优势和影响事件的能力。’网络实力可以用于在网络空间内达到想要的结果，或者，它可以利用网络工具在网络空间之外的领域制造想要的结果”。[21]

由于互联网具有跨国特征，各国政府已经意识到国际合作的必要性。众所周知，斯坦福大学教授斯蒂芬·克拉斯纳（Stephen Krasner）将国际合作以制度的形式定义为“或隐晦或清晰的原则、规范、规则和决策程序的集合。围绕这些元素，各方的期望交集于某个特定的国际关系领域。”[22]重要的是，虽然国家是这种制度的关键参与者，但不是唯一的参与者。其他实体也发挥一定的作用，比

[17] Toure, 2011: 9
[18] UN ITU-T X.1205 “Overview of Cyber-security”: 2
[19] Nye, 2010: 16
[20] Clarke and Knake, 2010: 73
[21] Nye, 2010: 4 citing Kuehl
[22] Krasner, 1983: 2

如国际组织。一个国际组织可以代表一项制度,或者是某项制度的一部分。比如,联合国难民事务高级专员办公室(简称UNHCR)代表了以难民公约为核心的制度。与此同时,UNHCR仅是更宽泛的人道主义制度的一个组成部分,后者包括联合国儿童基金会(简称Unicef),国际红十字会等许多其他制度。

与早期的委托-代理理论不同,像迈克尔·巴尼特(Michael Barnett)和玛莎·芬尼莫尔这样的学者,他们的研究已经证明了国际组织有自己的思维,并且追求的目标与其委托方的需求有所不同。[23]这说明了国际组织必须被理解为代理者,不能仅仅视其为结构。国际组织存在的合理性来自于它们的专业知识、被委托的权威和/或道德的权威。它们通过利用其制度性资源和话语性资源从其委托方中诱导出服从。[24]而且,巴尼特和芬尼莫尔已经证明了国际组织的权力,和它们是如何在国际关系中运用其影响力的。两位学者强调国际组织通过以下三种方式行使权力:"(1)划分世界,将行动者和行动内容分类;(2)修正社会学领域中的定义;(3)在全球阐明和传播新的规范、原则和行为体"。[25]举个非常有说服力的例子,在很多国家"难民"这一范畴与安全事务直接相关。[26]在网络竞技场上,ITU秘书长与世界科学家联合会一道提出了另一种将"网络和平"提上议程的指导框架,与那些充斥了"网络威胁"和"网络战争"等措辞的文献形成了鲜明的对比。

Ⅰ.2.规范与规范周期的概念

斯图尔特·贝克(Stewart Baker)是国土安全部的首席政策助理秘书。他于2011年3月4日在一次题为"网络安全:数码世界中的法律、隐私和战争"的活动中指出:心理学研究表明,人类天性使我们认为必须惩罚那些违背了某项社会规则的人。政治科学家詹姆斯·马奇(James March)和约翰·奥尔森(Johan Olsen)指出,除符合逻辑的预期结果之外,还存在逻辑的适当性(logic of appropriateness)。

"人类行动者被设想为会遵循某些规则,这些规则将特定的身份和特定的情境联系到一起。行动者探寻个人行动的机会,其方式是评估当前身份和选择困境之间的相似之处,或者更普遍地说,自我的概念与情境的相似之处。行动包含唤起某种身份或者角色,并将这一身份或角色的义务与某一特定的情境联系起来。

[23] Barnett and Coleman, 2005: 597-598
[24] Barnett and Finnemore, 2004: 5
[25] Barnett and Finnemore, 1999: 710
[26] Barnett and Finnemore, 1999: 710-711; Barnett and Finnemore, 2004: 73-120

目的的设定与身份相关。”[27]

简言之，规范并非是一成不变的，并且可以随着时间的推移有所加强或减弱，包括那些调节国际事务的规范。最近一个规范侵蚀的案例是禁止酷刑的规范的出现。正如贝克暗示的，关键的问题是我们将选择什么样的规范来指导网络空间的行为。

芬尼莫尔和斯金克在其文章《国际规范动态与政治变化》中提出了其规范生命周期的概念。她们将规范定义为“行动者在某个给定的身份下适当行为的标准”[28]，并将规范生命周期划分为三个阶段：“规范出现（norm emergence）”之后，一旦到达某个临界点，其潜在的结果是“规范扩散（norm cascade）”，接下来是规范的内化（internalization）。[29]重要的是，她们指出一次规范扩散或者内化并非一个线性的过程，而且也不一定会完成整个过程。

正如我接下来所要描述的，管理网络空间的规范似乎还处在第一阶段——规范出现。这并不令人感到奇怪，因为网络空间本身是相当新鲜的事物。然而，在网络领域已经有一些新兴的规范。例如，克林顿政府和继任的布什政府都不愿批准侵入恐怖分子的金融系统以追踪他们，哪怕就在 2003 年伊拉克战争前夕。[30]而且，“我们实际上拥有目标，但不打算袭击它，这在核战策略中被称为‘保留目标集（withhold target set）’。这种政策假定或者说期望对手也会受到那些没有挑明的规则的约束。”[31]这样的条款是规范出现的早期信号，同时，如果这些条款为国际社会所共享，那么将成为对网络战争行为的有效制约。

关于规范出现的第一阶段，芬尼莫尔和斯金克指出，“第一阶段，也就是规范出现的这一阶段，典型的机制是由规范倡导者积极说服产生的。规范倡导者试图说服一大批关键国家（规范的领导者）接受新规范。”[32]而且，她们找出了新规范得以成功形成的两个要素：（i）规范倡导者，（ii）倡导者可以利用的组织性平台。[33]（哈佛法学院教授劳伦斯·莱斯格（Lawrence Lessig）在其《社会意义的管制》一文中使用“意义建筑师”一词，这或多或少与规范倡导者是同义词。

[27] March and Olsen, 1998: 951
[28] Finnemore and Sikkink, 1998: 891
[29] Finnemore and Sikkink, 1998
[30] Clarke and Knake, 2010: 202
[31] Clarke and Knake, 2010: 203
[32] Finnemore and Sikkink, 1998: 895
[33] Finnemore and Sikkink, 1998: 896

[34]类似地，密歇根大学名誉教授约翰·W·金顿（John W. Kingdon）使用的是“政策倡导者”一词，只不过他是在更广泛的意义上使用的。[35]）

1.3. 联合国的规范倡导者

自从大卫·米特兰尼（David Mitrany）功能主义——通常以简化的形式表述为“形式追随功能”——在国际关系理论中生根发芽，学术界对于国际组织的理解极大地向前发展了。大体上讲，一个国际组织是由一个负责做决定的政府间机构全体会议和一个负责实施决定的官僚机构组成。属于前者的人员是外交官，属于后者的是工作人员或者国际公务员。在更为近期出现的一些文献中，一些学者已经证明了国际组织的官僚机构在某些条件下是具有自主性的行为体。从本质上讲，形式有其自己的生命。[36]

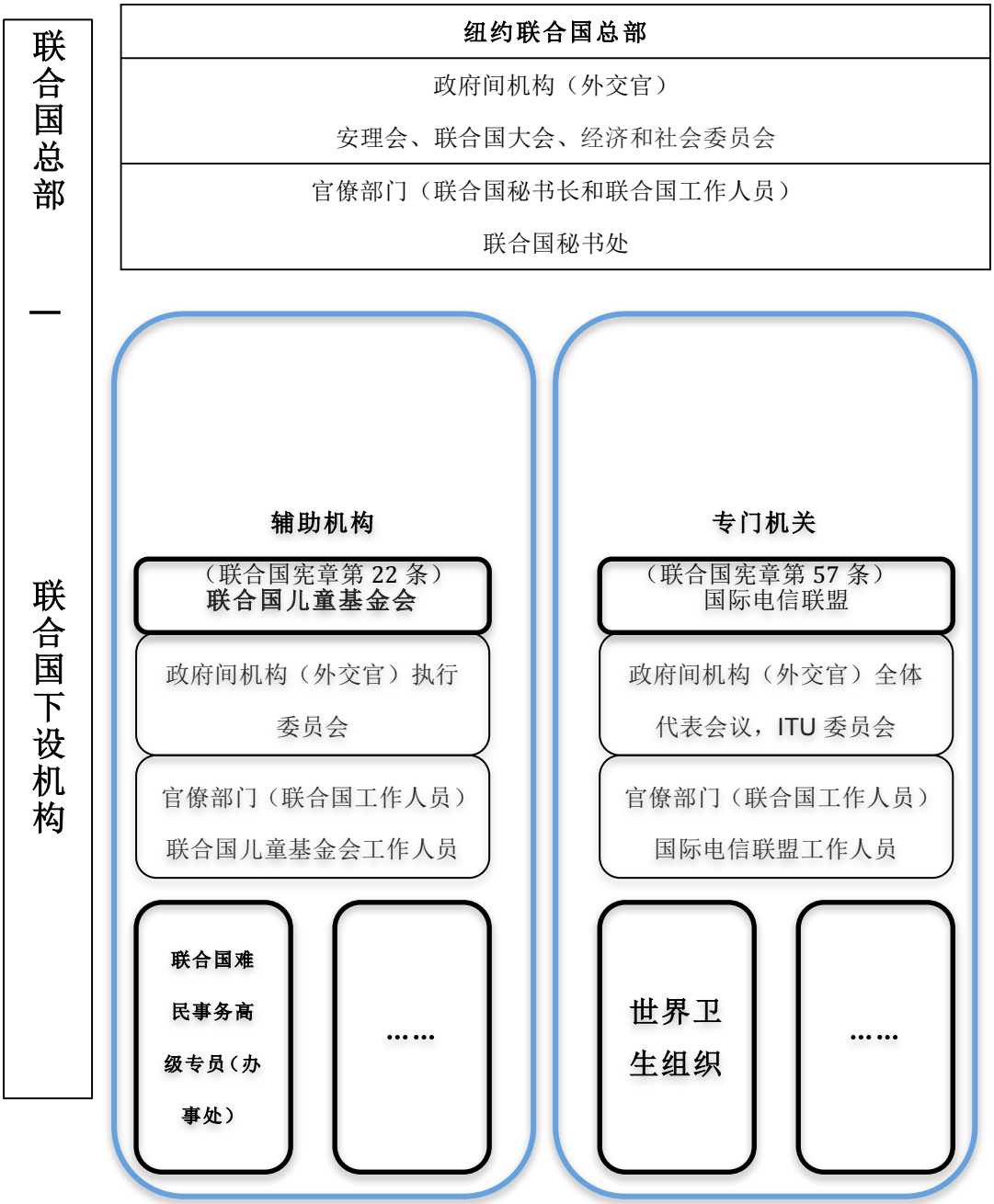
因此，规范倡导者是政治家、外交官、军队服役人员和学界人士。从本质上讲，任何拥有足够资源来发挥影响力的人都可以当一名规范倡导者。就此而言，联合国十分重要。第一，作为外交活动结果的规范和制度在联合国产生。第二，联合国官员本身就是政策倡导者。下文在讨论 ITU 秘书长所支持的网络和平行动时，联合国官员作为规范倡导者的角色将进一步阐明。这一点正好符合芬尼莫尔和斯金克的观点——她们将联合国描述成可以作为组织性平台发挥作用的常设组织。她们强调，这样一个平台常常受制于各种不同的，有时甚至是相互冲突的议程。[37]

联合国的核心是《联合国宪章》。《联合国宪章》提供了法律框架，成为将不同实体之间的关系概念化的最准确表达。联合国政府间实体由三部分组成:(1)安全理事会，由 192 个成员国中的 15 个组成；(2）经济和社会理事会（简称 ECOSOC），共有 54 个成员国参加；（3）大会，包括全部 192 个成员国。外交官是这些机构中的行动者。这三个机构的官僚部门是大家所熟知的联合国秘书处，由联合国秘书长领导。外交官持其所属国政府的护照，而联合国工作人员持单独的蓝色联合国护照，以证明政府间机构与官僚机构之间的区别。

这种两级组织架构的设计在联合国下设机构中也存在。这些下设机构是联合国架构的一部分，根据《联合国宪章》第二十二条，它们既可以是一个辅助机构，

[34]Lessig, 1995
[35]Kingdon, 2003
[36] Barnett and Finnemore, 1999, 2004
[37]Finnemore and Sikkink, 1998: 899

也可以根据《联合国宪章》第五十七条作为一个专门机关。下图形象地显示了联合国的组织结构关系。要记住,任何一个单独部门的结构都可能与整体结构不同。这种依法而建的等级制解释了为什么我的分析仅限于关注《联合国宪章》的核心部分，比如安理会、ECOSOC 和联合国大会等政府间机构。其他政府间机构的动态关系超出了本文范围，可以作为未来的研究对象。其他机构包括 ITU 的管理机构，联合国犯罪大会，以及《联合国打击跨国有组织犯罪公约》缔约方会议等。联合国毒品和犯罪问题办公室（简称 UNODC）的政府间机构也是本文关注的对象，因为它们是 ECOSOC 的功能委员会。为达成本文的研究目的，我效仿芬尼莫尔和斯金克，将其他机构作为组织性平台来参考，但这不包括 ITU。如下图所示，ITU 的角色是双重的。



I.4. 规范与国际法

根据《联合国宪章》第二十二条“联合国会员国同意依宪章之规定接受并履行安全理事会之决议”，安理会是唯一一个有权制定约束性国际法律的合法机构。另一方面，根据《联合国宪章》第十条和第十二条，联合国大会只能行使建议权。然而，联合国大会依然很重要，原因何在？

自法学家洛德·麦克奈尔（Lord McNair）所著《条约的功能和不同的法律性质》于 1930 年出版以来，部分学者已经就国际法中软法和硬法的区别展开讨

论。根据《国际法院规约》第三十八条第一款第一项规定，软法以成文法的形式出现，但不作为法律来源。[38]根据法学教授艾伦·E. 波义耳（Alan E. Boyle）的研究，软法和硬法在以下三个方面有所不同，因为软法：第一，不具有约束性；第二，争端的解决方式是非强制性的；第三，由一般性规范和原则组成。但同时软法以影响国家活动为目的。[39]亚利桑那州立大学法学教授肯尼斯·W. 阿伯特（Kenneth W. Abbott）和芝加哥大学政治学教授邓肯·J. 斯奈德尔（Duncan J. Snidal）将软法的这些特性归结为在约束力、精确性和委托性上的差异。[40]下文将要讨论的联合国大会决议即属于软法的一种。然而，ECOSOC 的决议却没有那么重的分量，这是因为 ECOCOC 的会员资格是有限的，因此它不具备代表联合国所有会员国的联合国大会那样高度的合法性。

因此，联合国大会的活动符合我们从软法的文献中预期到的情况。这些文献指出，软法有时优于硬法，这是因为“需要刺激那些尚未完成的发展”，以及“创建一种初步的、灵活的制度，或许可以为各个阶段的发展提供条件。”因为“通常的情况是，在某次会议上确定下一份文本的非条约约束性标准（non-treaty-binding standard）[赫尔伯格（Hillgenberg）使用这个词作为软法的同义词[41]]之后，随着对该文本认识的加深，它将会逐渐成为一项具有约束性的、也可能是一项‘硬性的’义务。”[42]

总之，关于软法和硬法的研究证明了软法在国际关系中发挥着重要的作用。软法可以发展成为一项国际性条约，或者作为一项条约的补充而存在。芬尼莫尔和斯金克在她们的著作中指出，“理解哪些规范可以成为法律(‘软法’或‘硬法’)以及如何遵守这些法律似乎将是法律与国际关系双重领域的又一重要研究课题”，因为这些法律性规则指导并决定了政治行为体的行为。[43]希望本文下面的分析对于理解规范如何治理网络空间有所帮助。

II. 网络安全与联合国

网络安全规范在联合国出现的过程可以划分为两个主要的谈判派别：一个是关注被我简称为“政治-军事”问题的派别，和一个关注经济问题的谈判派别。

[38]Chinkin, 1989; Hillgenberg, 1999
[39] Boyle, 1999
[40] Abbott and Snidal, 2000
[41]Hillgenberg, 1999: 500
[42]Hillgenberg, 1999: 501; see also Boyle, 1999: 904; Chinkin 1989: 856, Abbott, and Snidal, 2000: 447. 国家选择软法而不是硬法安排的原因更详细的解释，参见 Abbott and Snidal, 2000.
[43]Finnemore and Sikkink, 1998: 916

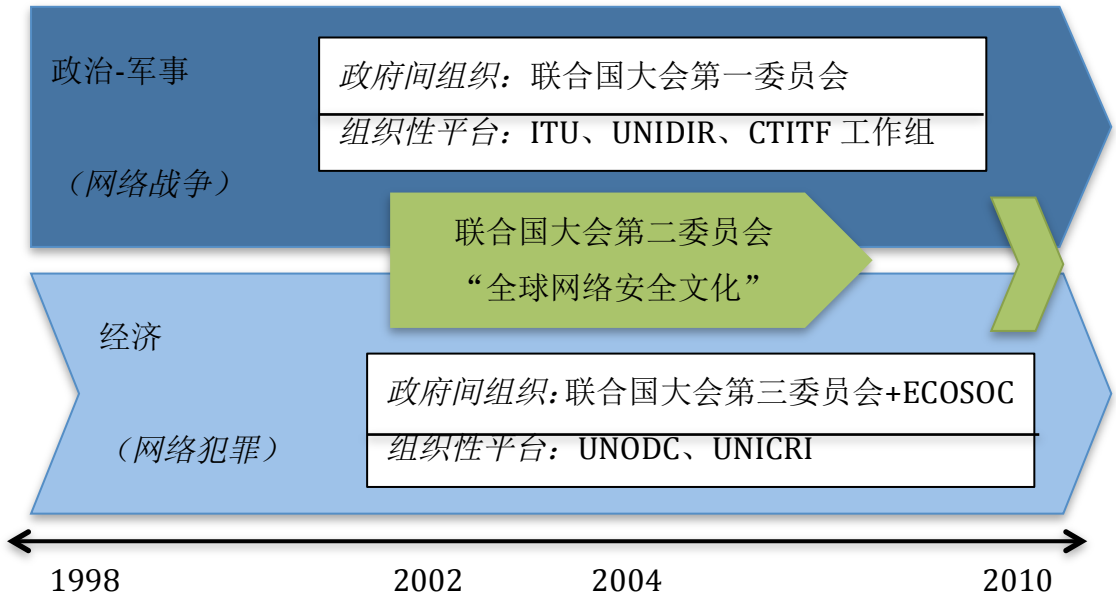
用联合国的话来说，政治-军事派别关注的是“[信息]技术和手段可能会被用于破坏国际稳定与安全的宗旨的目的，并对各国的安全产生不利影响”。[44]另一方面，经济派则关心“信息技术的非法滥用”。[45]

这两个派别换个词来称呼，则分别是网络战争和网络犯罪。克拉克和康科将网络战争定义为“代表或支持某个政府的非授权侵入，即侵入另一个国家的计算机或网络，或者任何其他影响计算机系统的活动。侵入的目的在于增加、改变或者篡改数据，或者干扰或损坏一台计算机、一台网络设备或一个计算机系统所控制的目标”。[46]奈提出了一些补充性的观点，这些观点从更广泛且非法律性的角度定义了网络战争。[47]

有一些人反对使用这四个术语（分别是：政治-军事派别、经济派别、网络战争和网络犯罪，——译者注），但是出于本文的研究目的，我将不对此进行深入讨论。然而，我想要指出的是，除了这些有关定义的问题，还有一系列关于“战争”或者“犯罪”是否能够充分地描述网络空间的某些行为等非常重要的问题。这些问题尤为重要，因为网络空间中领土缺失这一问题对于法律上战争与战场的传统定义具有关键意义。

[44] UN General Assembly A/RES/53/70
[45] UN General Assembly A/RES/55/63
[46] Clarke and Knake, 2010: 227
[47] Nye, 2011

联合国网络安全规范出现过程：两个派别的模型

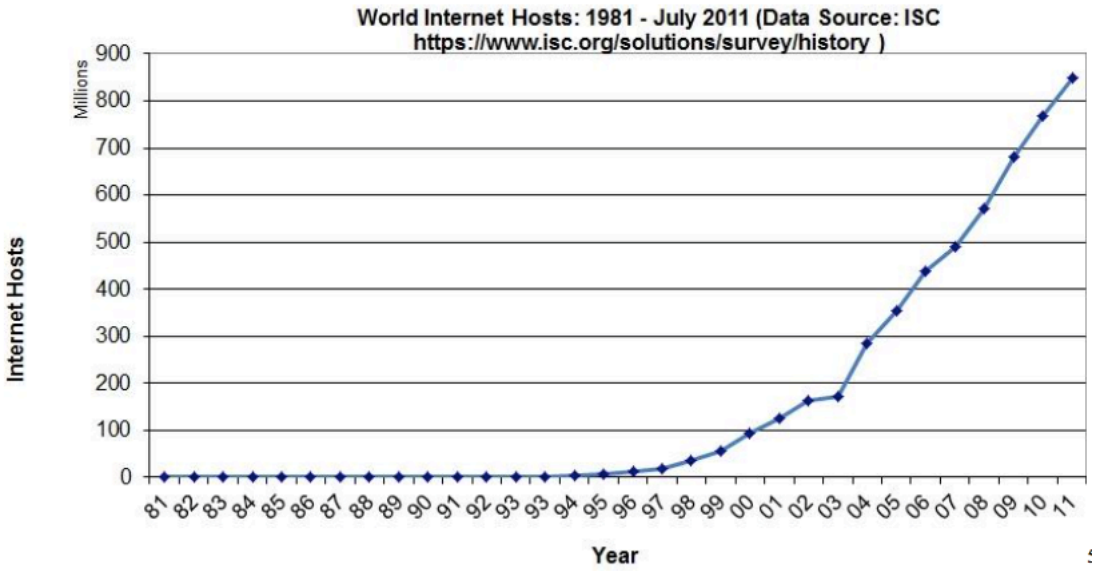


我们也可以增加第三个派别。这一派以 IGF 为中心，负责解决更广泛的互联网治理问题。这些问题涉及到很多机构，包括互联网名称与数字地址分配机构等等。然而，这些谈判并未直接处理网络安全问题，且 IGF 成立至今也仅只有五年的时间。这就是为什么本文第三部分将简要地讨论这些谈判，以呈现出更全面的情况，但不将其作为一个单独的分析单元和流派来讨论。另外，ITU 将联合国儿童基金会（Unicef）列为儿童在线保护行动的合作方之一。然而，在网络安全问题上，Unicef 的介入基本上是非常有限的。[48]

至于时间轴为什么从 1998 年开始：首先，1998 年是俄罗斯政府向第一委员会提出决议的头一年。一些关于计算机犯罪的决议在 1998 年之前就被采纳了。例如，联合国大会第 55/63 号决议提到了 1990 年召开的第八届联合国预防犯罪和罪犯待遇大会。然而，我关注的是第一委员会，因为在 1998 年恰恰出现了另一项重要的发展，即于 20 世纪 90 年代后期出现的互联网开始的指数性增长，如下图所示（这也是为什么通常将 1995 年当作“元年”。[49]）。这一增长与互联网用户数量的指数性增长相关，而用户数量的增长带来了更高程度的相互依赖以及相应升高的潜在威胁程度。

[48] Unicef; UN ITU “Child Online Protection”
[49] Carr, 2010

世界互联网用户：1981 年至 2011 年 7 月（数据来源：ISC https://www.isc.org/solutions/surey/history）[50]



联合国政府间机构的成员国就网络安全进行的谈判可以用《原子科学家公报》对罗纳德·德贝特（Ronald Deibert）采访中的一部分摘录来概括。德贝特是政治科学教授，也是多伦多大学公民实验室的主任。

“《原子科学家公报》：美国已推动了在预防犯罪方面更广泛的合作，俄罗斯也呼吁实施‘网络军备控制。’您认为这可以实现吗？

德贝特：俄罗斯已开始推动网络空间的军备控制，或者说信息武器的控制。大多数人对此不屑一顾，认为这不够真诚，对此我基本同意。大多数观察家将这些举动视为俄罗斯努力限制美国在网络领域方面的优势地位。但俄罗斯更加关心的是异议分子和人权组织在互联网上进行的颜色革命和动员——并试图消除美国支持这类社会动员的能力——而非完全关心保护其互联网领域。尽管如此，我认为网络军备控制是值得推举的。如果我任职于某个外交部，我也会借此契机来公开讨论国家之间的克制与合作，并回过头来讨论网络空间的规则应该是什么”。[51]

或者，如《纽约时报》所言：

[50] Wikipedia “The History of the Internet”
[51] Deibert, 2011: 6

“据美国官员所说，俄罗斯人主要关注三个相关的议题[…]除了继续努力禁止攻击性网络武器，俄罗斯还坚持呼吁禁止‘网络恐怖主义’，他们认为这是一个关乎主权的问题。美国官员对这个问题则有不同看法，认为俄罗斯是在试图限制‘政治破坏言论’。俄罗斯还拒绝接受欧洲委员会《网络犯罪公约》的部分内容，声称这违背了俄罗斯宪法，因为该《公约》允许外国法律执行机构在俄罗斯境内进行互联网搜索。”[52]

《华尔街日报》的记者塞欧翰·高曼（Siobhan Gorman）在他 2010 年 6 月的一篇文章中也指出，美国认为，考虑到条约无法阻止俄罗斯和中国这样的国家利用第三方机构来规避该条约，因此该条约是不成熟的。[53]

安理会对网络安全工作的介入很大程度上局限于“打击以恐怖主义目的使用互联网工作组”，这个工作组是联合国反恐执行工作队（简称 CTITF）的一个部分。在安理会的决议中，例如 2008 年格鲁吉亚决议，都没有提及网络方面的内容。（2007 年爱沙尼亚和 2010 年伊朗都没有决议。）

以一个简单的标题“网络安全：威胁与挑战的兴起”，ECOSOC 启动了其 2010 年的工作。[54]ECOSOC 的两个功能委员会，麻醉药品委员会和预防犯罪和刑事司法委员会，都已开始着手处理违法使用网络空间的问题。

联合国大会已经进行了许多关于成员国行为管理规范的活动和讨论，例如大会决议的两份附件（参见附录）中的要点。大会六个委员会中的三个都已就网络安全决议草案进行了谈判。和所有决议草案一样，这些草案接下来会递交给大会全体会议，并在秋季的年度大会上决定通过与否。这些决议草案是由下面几个委员会递交的：

第一委员会（裁军和国际安全委员会），处理裁军和国际安全相关问题；

第二委员会（经济和财政委员会）处理经济问题；

第三委员会（社会、人道主义和文化委员会）处理社会和人道主义事务。

截至目前，在网络相关事务方面共成立了五个政府专家组。第一个专家组于 2004 年由大会第一委员会组建。之后第一委员会组建了第二个专家组，并且该

[52]Markoff and Kramer, 2009

[53] Gorman, 2010

[54]Toure, 2011: 92; ECOSOC “2010 ECOSOC General segment briefing”

小组于2010年发布了报告。2004年，ECOSOC建立了一个关于身份相关犯罪问题的政府间专家组，该小组现已逐步发展为核心专家小组之一。ITU建立了一个高端专家组，该小组在2007年制定了网络安全议程。联合国预防犯罪和刑事司法委员会在2010年建立了一个不限成员名额的政府间专家组，致力于打击网络犯罪。

在谈判中，成员国通过利用联合国的各个组织为平台，在议程上展开竞争。这也为联合国网络安全活动的高度碎片化做出了解释。正如我下面的分析所证明的那样，有趣的专业知识弥散在这个体系之中。ITU将联合国网络安全工作的相关组织分类如下：

（1）打击网络犯罪：ITU和UNODC；

（2）能力建设：ITU、UNIDIR和UNICRI；

（3）儿童在线保护：ITU、Unicef、UNICRI、UNODC。[55]

然而，这种分类并不全面。比如，为什么儿童在线保护行动和UNODC的法律执行官员培训不能算作能力建设的一种,或者为什么打击网络犯罪中没有提到联合国区域间犯罪和司法研究所（简称UNICRI）。我这篇文章的第二部分将做一个更全面的情况介绍。

一般说来，ITU和UNODC被认为是联合国网络安全和网络犯罪方面最重要的两个机构。[56]这就是为什么ITU的秘书长和UNODC的执行理事决定为这两个机构建立正式的合作关系。除此之外，联合国驻纽约秘书处通过其政治事务部和联合国裁军研究所（简称UNIDIR）协助之前提到的CTITF工作组开展工作。而UNICRI关注的是网络犯罪。

分析这些组织的工作很重要，这不仅是出于一种组织性平台的视角，更是因为除了成员国之外，联合国的官僚自己也是规范倡导者的一部分。芬尼莫尔和斯金克提醒我们，“规范不会凭空而出；规范是通过代理人积极建构而形成的，这些代理人对于其共同体中哪些行为是适当的或者可取的有着强烈的认识。”[57]这些代理人拥有影响力，这是因为他们拥有设定议程的权力，以及“框定”或者“‘创

[55] UN ITU, March 2010: 36
[56] UN ITU“PowerPoint Presentation”
[57]Finnemore and Sikkink, 1998: 896

造’议题的权力，其方式是利用语言来命名、解释和改编议题”。[58]正如巴尼特和芬尼莫尔所强调的，国际组织自主行动的官僚机构属于规范倡导者的一部分。这就是为什么这些官僚机构既是一项制度中的积极分子，也是创造一项制度的积极分子。如下文所描述的，ITU 是一个很好的例子，它说明了一个联合国的官僚机构如何作为一名规范倡导者独自行动。

下面的章节将主要分析前面提到的派别。如上面的表格所示，对每一个派别的分析可以分为两个小部分。首先，我关注会员国及其在政府间实体中的谈判。其次，观察会员国如何将联合国各组织的官僚机构作为组织性平台加以利用。

II.1. 政治-军事派别：网络战争

克拉克在他的书里写道：“美国几乎是在单打独斗地阻止网络空间的军备控制。多少有些讽刺的是，俄罗斯是主要的支持者[……]自从克林顿政府首次拒绝了俄罗斯的提案，美国自始至终都是网络军备控制的反对者。或者完全坦率地说，我或许应当承认，我拒绝接受俄罗斯的提案[……]也许美国是时候重新评估自己在网络军备控制上的立场，并自问以通过国际协议来实现军备控制是不是会获得或多或少的益处”。[59]

这场辩论是联合国大会第一委员会就“安全背景下信息和电信领域的发展”展开的谈判的中心议题，也是本文这一章节的第一部分内容。第二部分将分析著名的 UNIDIR 和 ITU 是如何在此背景下被作为组织性平台来利用的。

II.1.1. 联合国大会第一委员会

俄罗斯政府首次向第一委员会提交“安全背景下信息和电信领域的发展”决议草案是在 1998 年，并且在此后的每一年都再次提交。这份决议草案以时任俄罗斯外交部长的伊格·伊万诺夫（Igor Ivanov）于 1998 年 9 月 23 日递交给联合国秘书长的一封信为基础。信中要求将这份决议草案传播出去。[60]2001 年至 2007 年担任俄罗斯国防部长的谢尔盖·伊万诺夫（Sergey Ivanov）稍后发表声明，“俄罗斯想要建立国际法律制度以防止信息技术被用于与确保国际稳定和安全背道而驰的目的”。[61]

[58]Finnemore and Sikkink, 1998: 897
[59] Clarke and Knake, 2010: 218-219
[60]Streltsov, 2007
[61] Ford, 2010: 65

正如克拉克所暗示的，俄罗斯和美国主导了联合国大会中的交锋。这一点可以从决案的提出和支持，以及投票模式中窥见端倪。俄罗斯呼吁出台一项网络军备控制的协议，而美国政策立场方面的进展正如一位外交官所表达的，“适用于动能武器的法规也应该同样适用于网络空间的国家行为”，与此同时努力在法律执行机构之间增进国际合作。[62]考虑到过去两年中国针对网络安全问题在媒体上所引起的特别关注，中国在大会上对该问题的相对沉默值得注意。

第一阶段：1998-2004 年——网络规范出现的第一阶段。1998 年的决议草案于 1999 年 1 月 4 日作为第 53/70 号决议被通过。其基础是之前的一份文件，“科学和技术在国际安全、裁军及其他有关领域的作用”（A/53/576，1998 年 11 月 18 日）。关于“国际计算机安全协议”[63]的决议的关键内容如下：

-首次提出信息和通讯技术在军事方面的潜能[64]，并且高度关注技术或被用于“不符合维护国际稳定与安全的宗旨”[65]（俄罗斯的立场）

-提到有必要防止网络犯罪和网络恐怖主义（美国的立场）

-吁请成员国通报联合国秘书长其关于“国际原则”的“定义”与发展的看法（关于下一阶段的执行部分段落）。

2010 年的版本对这一份决议草案做了两处关键的改动。也是在 2010 年，美国首次成为该决议草案的共同提案国，而在 2005 至 2008 年期间美国一直投反对票。这两处改动分别是：

-删减去出处，并试图提出一些定义，这些定义可以作为制定网络军备控制协议的第一步

-用“国际观念”和“可能的措施”等提法代替“国际原则”的提法

大会未经表决通过了这一问题的第一份决议，即第 53/70 号决议。然而，推动制定一份国际协议的努力却遭到美国怀疑主义的抵制，而欧洲国家也怀疑这样一份协议可能会在日益重要的信息和电信安全的伪装下被用于限制信息自由。哈德逊研究所资深专家克里斯托弗·A. 福特（Christopher A. Ford）在他关于俄罗斯网络政策的分析中得出如下结论，“在应对信息战争以及信息战争在网络空

[62] Ford, 2010: 67; Markoff, 2010
[63] Markoff, 2010; for literature on a cyber arms convention see for example Geers, 2010; Ford, 2010.
[64] Streltsov, 2007
[65] UN General Assembly A/RES/53/70

间的应用方法中，俄罗斯过多地强调对大众媒体的控制，同时也意在影响国内外的观念。[66]他举出的例证是俄罗斯政府在20世纪90年代试图实行直接审查制，以及2000年颁布《信息安全条令》。[67]

同时，根据俄罗斯联邦国防部专家谢尔盖·科莫夫（Sergei Komov）、谢尔盖科·罗特科夫（Sergei Korotkov）和伊戈尔·戴莱夫斯基（Igor Dylevski）的说法，鉴于美国仍然是技术领域的领先者，美国没有限制技术使用的必要和动机。这几位专家在2007年的一篇题为“在普遍认可的国际法原则的背景之下，从军事角度保证国际信息安全”的文章中强调了他们的上述观点。此文刊登于UNIDIR的刊物《裁军论坛》中。[68]福特指出，“俄罗斯惧怕与美国展开一场网络军备竞赛，这一普遍的看法是准确的。一些俄罗斯的官员也已对此发表了很多看法。”[69]克拉克和康科的书中提到军事革命和1990至1991年海湾战争中信息技术的作用时，记录了中国官员也持类似的看法。[70]

第二阶段：2005-2008年——倒退，动态过程的信号。2005年，第一委员会发生了一次重要的转变。俄罗斯提出的决议草案获得通过，但却是历史上首次使用记名投票的方法。美国是10月28日那天唯一一个投票反对该决议的国家。[71]当时恰逢乔治·W·布什总统的第二任期，也是2005世界首脑会议失败之后联合国和美国关系的历史低点。2005年美国投票反对该决议之后，到了2006年，就不再是俄罗斯联邦单独支持决议草案（A/C.1/61/L.35）了。相反，中华人民共和国、亚美尼亚、白俄罗斯、哈萨克斯坦、吉尔吉斯斯坦、缅甸、塔吉克斯坦以及乌兹别克斯坦等国共同支持该草案，而在随后的几年，其他一些国家也加入了支持的行列。[72]有趣的是，如下面关于支持度的表格所示，美国的反对实际上可能提升了成员国对该问题的重视程度，从而为多边支持决议的局面做了铺垫。

成立于2004年的首个政府专家组定于2005年提交了一份报告，但专家组最终未能形成统一的立场，这迫使秘书长不得不总结：“鉴于所涉问题的复杂性，在编写最后报告时未能达成共识。”这一结果在联合国是相当不同寻常的。联合国的活动通常是在局面已经清晰可见之后才开始启动，即至少存在某些所有人都同意的最低程度的共识，这样即便行动失败，每个人都还可以保持颜面。这个专

[66] Ford, 2010: 59
[67] Ford, 2010: 60+61
[68] Komov et al, 2007
[69] Ford, 2010: 62
[70] Deibert, 2011: 3
[71] UN General Assembly A/60/452
[72] UN General Assembly A/C.1/61/L.35; UN General Assembly A/61/389

家组是由来自15个国家的政府专家组成：白俄罗斯、巴西、中国、法国、德国、印度、约旦、马来西亚、马里、墨西哥、大韩民国、俄罗斯联邦、南非、大不列颠及北爱尔兰联合王国、和美利坚合众国。他们举行了三次会面，一致选举俄罗斯联邦的安德烈·A·克鲁茨基赫（Andrey V. Krutskikh）担任主席。

A.A.斯特雷索夫（A. A. Streltsov）是俄罗斯在政府专家组会议代表中的一员，也是俄罗斯联邦密码学会的成员，根据他的说法，“主要的障碍是下面这个问题，即国际人道主义法律和国际法在信息与通信技术（简称ICT）被恶意使用为政治军事目的服务时，是否可以有效管制国际关系中的安全问题。政府专家组的工作并非毫无价值，专家组的工作成功地提升了相关问题在国际议程中的地位。”[73]

也是在这个时期，随着分布式拒绝服务器（简称DDoS）攻击爱沙尼亚，网络战争于2007年首次登上头条，并在2008年格鲁吉亚-俄罗斯战争期间再次成为头条。（这提醒我们，两次被描述为“网络战争”的事件也依赖于规范的逐步出现，以及正在形成中的关于如何将这类事件进行分类的共识。例如，目前对于DDoS 到底是一次网络攻击，还是受第一修正案保护的某种形式的抗议，目前仍然存在争论。[74]这场持续进行的争论聚焦于该事件的意图。另一方面，震网效应看起来比传统的攻击更具破坏性。[75]这意味着，如果一种类似的技术不是用于破坏工业设施而是造成直接的身体伤害，那么其后果就会是另一个关键的因素。简言之，这场辩论既是关于规范的，也首当其冲地是关于如何对世界进行分类的。）

第三阶段：2009-2011年——再次前进。从2009年10月开始，决议草案重返2005年之前的情形，在第一委员会未经投票而获得通过。布什政府已由奥巴马的政府接任。奥巴马总统追求的“重置”的政策不仅针对俄罗斯，也针对联合国。事实上，2009年11月《纽约时报》报道：

“拉迪斯拉夫·P·舍尔斯丘克（Vladislav P. Sherstyuk）将军是俄罗斯安全理事会的副秘书长，也是相当于美国国家安全局的俄罗斯安全部门的前任领导人。由他带队的代表团在华盛顿和来自美国国家安全委员会、国务院、国防部和国家安全部的代表举行了会晤。熟悉这些谈话的官员声称，双方就弥补长期以来两国间的隔阂取得了进展。事实上，两周之后在日内瓦，美国同意与来自联合

[73] Streltsov, 2007: 6+7
[74] 我感谢奥利弗·里德提供这个想法。
[75] 我感谢约瑟夫·奈提供这个想法。

国裁军和国际安全委员会的代表就网络战争和网络安全进行讨论。”[76]

而且，2010 年 1 月，奥巴马政府为了使各方联系更加紧密，提出了一份立场文件。[77]当年的晚些时候，第二个政府专家组终于提交了报告。这一次政府专家组终于达成了共识，声称“信息安全领域当前和潜在的威胁是 21 世纪面临的最严峻的挑战。”专家们认为罪犯、恐怖主义者和国家都是潜在的犯罪者。个人、商业、国家基础设施和政府则被定为潜在的受害者。随着国家逐步提高网络战争能力，威胁已达到可以将“国际和平与国家安全”置于危险之中的程度。专家们承认，网络空间存在归属问题并且具有“双重使用”的特征，这与“互联网是中性的”这一认知保持一致，互联网的使用方式取决于其用户的意图（并会产生无法预期的结果）。报告还提到了目前打击非法使用信息技术和创造一种“全球网络安全文化”的努力。关于“信心构建并采取其他措施以减少由 ICT 干扰所引起的误解”，专家组提出了以下五点建议：

“1. 各国之间应进一步对话，以讨论关于国家使用信通技术的准则，降低集体风险并保护关键的国家和国际基础设施；

2. 加强信任建立、网络稳定和减少风险的措施，以应对国家使用信通技术过程中的任何问题，包括在国际争端中利用信通技术交换国家意见；

3. 就国家立法及国家信息和通信技术安全战略和技术、政策和最佳做法进行信息交流；

4. 确定支持欠发达国家相关能力建设的计划措施；

5. 积极制定与大会第 64/25 号决议有关的共同术语和定义。”[78]

来自美国和俄罗斯的代表，米歇尔·G·马科夫（Michele G. Markoff）女士和安德烈·A·克鲁茨基赫先生是仅有的两位来自首个政府专家组的专家。他们也是第二个政府专家组的成员，而后者被同时选举为两个小组的主席。马科夫先担任了政治军事事务局国际重要基础设施保护部门的高级协调员，后又担任了国务院网络事务办公室的高级政策顾问。克鲁茨基赫先担任了裁军与安全事务部副主任，后任职于俄罗斯联邦外交部新挑战与威胁司。有趣的是，爱沙尼亚和以色列加入了这个 2009 年新成立的专家组。爱沙尼亚曾是第一个遭受大规模 DDoS

[76] Markoff and Kramer, 2009
[77] Markoff, 2010
[78] UN General Assembly A/65/201

袭击的国家，而以色列被认为是震网的潜在设计国家一。[79]

也是在同一时期，重要的维基解密文件和震网出现了，而美国有史以来首次决定加入第一委员会俄罗斯决议草案的共同提案国的行列。这引发了克拉克对于这一问题的最新思考，他在书中这样概括，“或许我应该承认我拒绝接受俄罗斯的提案[……]美国几乎是联合国唯一一个拒绝网络谈判的国家，我们说不行[……]，而且我们十多年来一直坚持拒绝这一提案[……]对于美国而言，或许现在是时候重新评估其在网络军备控制上的立场”。[80]第 65/41 号决议还包括一个新的段落，要求秘书长于 2012 年建立一个新的政府专家组，并在 2013 年第 68 届会议上递交报告。然而和第一阶段不同的是，这一决议不仅得到俄罗斯的支持，还得到了包括中华人民共和国在内的 36 个国家的支持。[81]

媒体是这样报道这些事件的：华盛顿邮报在题为“15 个国家同意开始就降低网络战争的威胁展开合作”的文章中写道，“包括美国、中国和俄罗斯在内的国家首次表露愿意参与到降低互相攻击计算机网络的威胁之中”。这位记者提到，“俄罗斯人在 1998 年提出了一份协议，这份协议禁止网络空间为军事目的所用”，他引用罗伯特·康科的话，认为新的发展是“奥巴马政府外交接触策略的一部分”，因为用奥巴马政府官员的话说，“国际上对于应对风险的需要有了更深的认识”。[82]

奈对新环境做了以下估计，

“在超过十年的时间里，俄罗斯一直在为更广泛的互联网国际监督寻找协议，以阻止在发生战争时激发恶意代码、电路欺诈或嵌入。但是美国人一直争辩说阻止进攻的措施也会损害对目前攻击的防范，而且也不可能得到证实或执行。此外，美国抵制使集权政府互联网审查合法化的协议。然而，美国已经开始与俄罗斯展开正式讨论。甚至连一项信息使用国际法的支持者们也怀疑，考虑到未来技术的多变性，一项类似于《日内瓦公约》的多边协议是否能够包含确切和细致的规则还有待考证，但支持者们也认为想法类似的国家可以公布自我管制规则，而这些规则未来可能发展成规范。”[83]

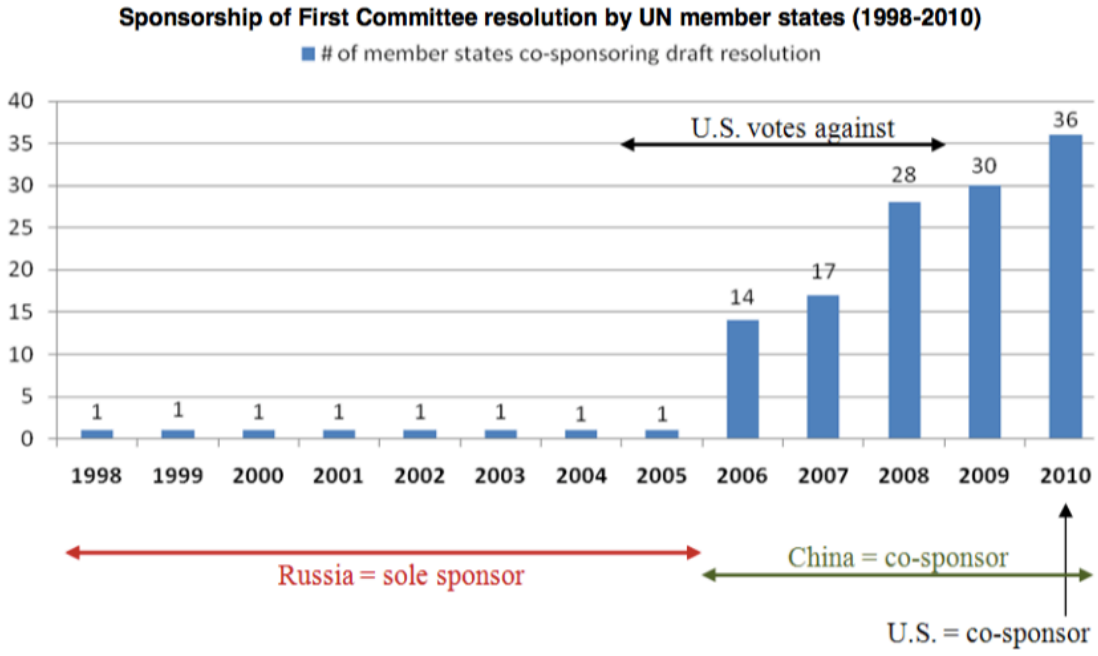
最新动态是俄罗斯、中国、塔吉克斯坦和乌兹别克斯坦四国政府递交给联合

[79] Broad et al, 2011
[80] Clarke and Knake, 2010: 218-219
[81] UN General Assembly A/65/405
[82] Nakashima, 2010
[83] Nye, 2010: 18

国秘书长一封联合信。信中包括了一份草案，即“信息安全行为国际准则”（以下简称《行为准则》，——译者注）（见附录）。

在一份初步分析报告中，美国对外关系委员会的西格尔•亚当（Adam Segal）强调，有几点事项可能充满争议。[84]第一，那些赞同《行为准则》的国家“努力[……]防止其他国家使用其资源、重要基础设施、核心技术和其他优势以削弱这些国家的权利。这些国家接受《行为准则》，意图在于独立控制信息和通讯技术，或者威胁其他国家政治、经济和社会方面的安全。”这看起来与互联网自由这一观念相冲突。互联网自由代表传统国际关系中的不干预原则，这一原则是解决很多分歧的基础。第二，《行为准则》的中心是国家以及多边合作。然而从传统上讲，互联网治理并不是由国家主导的，而是由私人部门和公民社会主导。这是一场“多边”（仅包括国家）与“多个利益攸关方”（包括国家、私人部门和公民社会）之间的辩论。（可以参见阿列克谢•西多连科（Alexey Sidorenko）的评论，http://censorshipinamerica.com/2011/09/24/russia-cyber-security-code-of-conduct/）

回过头看，下图根据第一委员会的活动分析绘制而成。此图证实了以下结论，即谈判是规范出现的早期阶段。

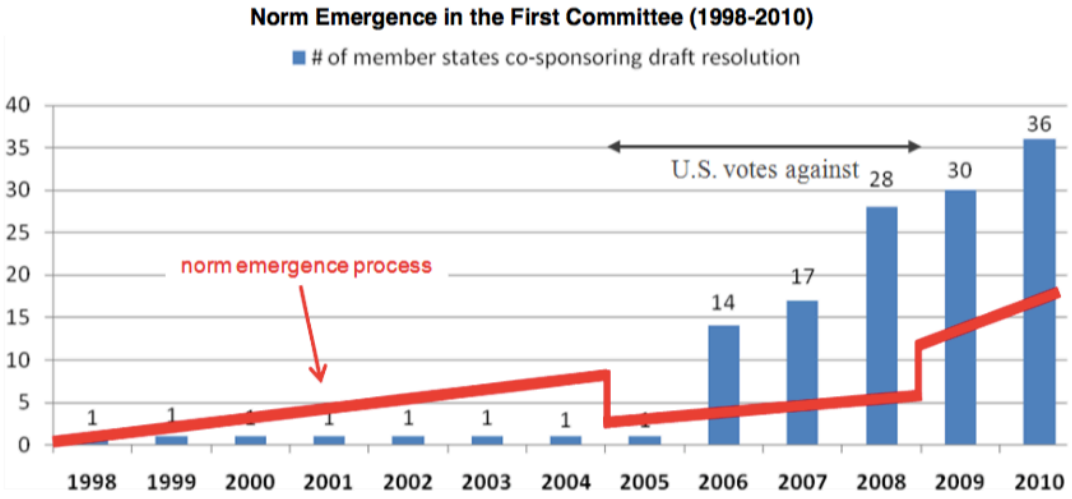


这篇报告并不是要找出影响规范出现的所有变量。出于本研究目的，支持网

[84] Segal，2011

络安全规范正在联合国出现这一结论的经验证据可以在定量和定性两种变量中找到。定量方面的一个例子是一份决议草案的共同提案国的数量，这意味着国际社会中对一项决议的兴趣和支持有所增加。另一个定量方面的证据是投票模式。如果某项决议未经投票而获通过，或者采用记名票的方式，或者甚至一些会员国投了反对票，那么这可以说明会员国对于某项具体决议所持的立场和重视程度。

我以这两个变量为例，来形象地说明第一委员会中规范如何出现。这一节下面的部分进一步详细地描述了规范出现的过程。然而，行动者、行动类型和时间轴的多样性削弱了图表展示的清晰度。希望下面的图表可以为第一委员会规范出现的过程提供一种基础性的理解。这张表强调的是规范出现的动态特征，正如2005-2008 年这段时期显示的，两股相反的趋势同时发生。首先，1998 年俄罗斯提出第一份决议草案之后，规范缓慢地出现。趋势线的斜率大于 0，这是因为决议草案每年都稳步地吸引足够的关注，但是直到 2005 年，俄罗斯仍然是该决议草案的唯一提案国。就在 2005 年，美国决定投票反对决议，因此打破了规范出现的静态势头。这一点可以通过当年规范出现趋势线的突然下跌直观地看出来。然而，美国在这四年期间的反对，也正是共同提案国的数量不断上升的时期，这就是为什么斜率在这一时期是大于 0 的，而且在 2009 年之后还有所上升。正是在 2009 年，美国决定允许决议通过而不再次投票。



显然，这只是一个非常基础的，用来测量和说明规范出现过程的模型。还有很多质的方面的变量也应该予以考虑，比如活动的类型、某项决议的实际内容、决议中使用的语言——“注意”、“欢迎”、“吁请”、“要求”等等——某些原则是否取得一致同意并有可能以附件的形式添加在决议中，某个政府专家组是否被成功建立以及是否确实提供了一份报告。另一个变量是处理问题的组织实体

的数量以及全部活动的数量，比如决议的数量、组织提供的项目和工作的数量。这些变量是本文行文的依据。

II.1.2. 组织性平台：ITU、UNIDIR 和 CTITF 工作组

联合国裁军研究所（UNIDIR）

位于日内瓦的 UNIDIR 是首批参与网络安全工作的联合国官僚机构之一。目前，德国资助一项题为“网络战争的角度：法律框架、透明性和信心构建”的持续性研究，目的是提升外交官对于该问题的认识，并激发进一步的多边讨论。UNIDIR 的合作方是汉堡大学的和平与安全政策研究所。[85]而且，两位 UINDIR 的成员，J•路易斯（J. Lewis） 和克斯廷•韦格纳德（Kerstin Vignard），在 2009 年 11 月至 2010 年 7 月期间担任 2010 年政府专家组的顾问。[86]值得关注的是，UNIDIR 举办了两次会议，都与大会第一委员会所讨论的内容有关：

1999 年，也就是俄罗斯向第一委员会提交第一份决议草案之后的那年，联合国裁军事务部主办了一场为期两天的讨论会，时间在 8 月 25 日至 26 日，题为“国际安全背景下信息和电信领域的发展”，与这个问题的决议名称相同。[87]来自超过四十个国家的七十余名参会者参加了这次会议。[88]讨论显示，对于威胁的估计以及诸如归属问题等普遍性问题的认识，在 1999 年已经广为人知。

同时，不同国家关心的首要内容不尽相同。一些国家认为网络犯罪和网络恐怖主义是首要问题，其他国家则更加关心网络战争。讨论是否应该为互联网增加限制或者支持互联网的物质基础设施，对这一问题本身也进行了讨论。讨论纪要强调了一种界定问题的方法，共分为三个部分：（i）军事事务方面的革命，（ii）以说服为重点的信息宣传，（iii）重要基础设施的保护和信心保证。[89]这看起来符合并且效仿了“信息-心理型”和“信息-技术型”的分类方法，这一分类方法被福特认为是俄罗斯解决网络安全问题方法的特征。[90]

2008 年，俄罗斯主办了第二次类似的会议。会议日期是 4 月 24 日至 25 日，主题为“信息通讯技术与国际安全”，目的是“审查信息和通讯技术恶意使用造成的既存的和潜在的威胁，讨论 ICT 带给国际安全的独特挑战和可能提出的相应

[85]UNIDIR “Research Project-Perspectives on Cyber War”
[86]UNIDIR “Research Project –GGE”
[87]UNIDIR “Conference-Developments”
[88] UNIDIR Summary
[89]UNIDIR “Conference-Developments”
[90] Ford, 2010: 57

对策”。[91]

除这些活动之外，UNIDIR 还在 2007 年《裁军论坛》第三份出版物中讨论了信息通讯技术与国际安全问题。[92]出版的文章聚焦于互联网治理、网络恐怖主义、重要信息基础设施、法律问题和军事方面的问题。第一篇文章是亨宁·维格纳尔（Henning Wegener）写的，他退休前是德国大使和世界科学家联盟信息安全常设监测小组的主席。在前面提到的 UNIDIR 的出版物中，他撰写了“网络和平”一章。除维格纳尔之外，还有两位学者以及四位俄罗斯政府的官员也在刊物上发表了文章。

国际电信联盟（ITU）

“国际电信联盟（ITU）是联合国的一个组织，主要负责网络安全实践方面的事务”。[93]这是一个条约性组织；事实上，这是联合国唯一一个以条约组织的身份就网络问题开展工作的组织。ITU 坐落于日内瓦，在联合国成立之前就存在了。根据联合国宪章第 57 条，ITU 后来作为一家专门的机构合并入联合国系统。它在设定技术标准方面发挥重要作用，并且由一个庞大的技术人员组织负责管理，这些人员有专门的关注领域，例如智能电网基础设施。[94]ITU 的秘书长每个季度向联合国秘书长递交一份威胁评估报告。该组织拥有一个专家数据库作为其资源基础，以防止网络袭击并维护全球网络安全议程。

从国际关系理论的角度看，ITU 在联合国网络安全工作中的作用是格外引人注目的，因为它不仅是一个为会员国所用的组织性平台，还是一个自主性的规范倡导者。ITU 的官僚机构代表，也就是将打击网络犯罪视为三项最主要职能之一的秘书长，[95]其活动超越了传统的委托-代理关系。

作为一个组织性平台并依据经典的委托—代理理论，在突尼斯召开的信息安全世界首脑会议要求 ITU 负责 C5 行动方针，即“在使用 ICT 方面构建信心和安全”，这一要求得到了 ITU 全体会议第 140 号决议的证实。[96]作为对突尼斯议程的回应，ITU 秘书长哈玛德·I·图埃（Hamadoun I. Toure）于 2007 年 5 月发布了全球网络安全议程。在 2007 至 2008 年间，一个高端专家组在发布《2008 年

[91]UNIDIR “Conference- ICT and international security”; UNIDIR Agenda
[92]UNIDIR “ICTs and International Security”
[93] CTITF May 2011: 7
[94] UN ITU Global Strategic Report, 2008: 95
[95] UN ITU “PowerPoint Presentation”
[96]Toure, 2011: 104

全球策略报告》之前举行了三次会议，该报告后来被压缩成一本 47 页的手册。[97]《全球策略报告》聚焦于五个领域，(i)法律措施，(ii)技术和程序措施，(iii)组织结构，(iv)能力建设，和(v)国际合作。ITU 称全球网络安全议程是一个“网络安全的国际性框架”。[98]

全球网络安全议程向 ITU 提出的建议包括为会员国提供可供采纳的立法模式，并在可能的情况下协助会员国使用布达佩斯《网络犯罪公约》作为立法范例。另一个建议是建立“网络安全就绪指数”，其基础是某些组织性结构，例如一位促进合作的国家领导人，或者一个国家的网络安全委员会，以及一个国家的计算机应急小组。ITU 还为国家基础设施保护提供了框架，并提议将下述问题概念化，即大会第 57/239 号决议中谈及的网络安全文化可以作何理解。[99]全球网络安全议程与反网络恐怖主义国际多边合作组织(简称 IMPACT)签署了一份理解备忘录，该组织是在马来西亚政府支持下于 2008 年成立的，被称为全球网络安全日程的实体家园。[100]正如前面提到的，ITU 还用示范语言制定了一套网络犯罪立法的工具，其中包括一些解释性的评论，可以作为网络犯罪法律一致化的基础。这套工具还概括出了一个矩阵，以对不同国家的法律规定进行比较。

作为一个自主性的规范倡导者，ITU 由于其秘书长所采取的某些行动而显得尤为突出。大体上讲，ITU 的策略可以分为两个方面：首先，ITU 试图推进其会员国提出的广泛议程。第二，ITU 关注具体的行动。至于第二点，以儿童在线保护为例，该行动已经被认为是一项值得所有国家认可并建立信任的尝试，这样社会化影响就能够潜在地产生积极的溢出效应，对更广泛的网络安全议程有所帮助。除此之外，2010 年在海得拉巴举行的世界电信发展大会上，ITU 秘书长提出了不在网络空间“先发制人承诺”，并提议各国“应该努力不让网络恐怖主义和袭击者在本国受到免于惩罚的庇护”。[101]这些言论仅是演说的部分内容，而且并不是对会员国的正式要求。值得关注的是，克拉克和康科在他们的《网络战争》一书中提出了类似的建议，声称“焦点在于不让网络攻击引发战争，而不在于一旦冲突已经开始再去限制网络攻击的使用，这一保证适用于所有国家，或只适用于那些作出类似声明或者签署协议的国家。”[102]

[97] UN ITU, March 2010
[98] UN ITU, March 2010
[99] UN ITU, March 2010: see graphs on p. 76+121
[100] Toure, 2011: v
[101] The Hindu Business Line, 24 May 2010; Pradesh, 25 May 2010; Wegener, 2011: 81
[102] Clarke and Knake, 2010: 239

同时，ITU 的作用不仅是各个国家的组织性平台。世界科学家联盟在联合国和 ITU 涉及到网络安全的活动中发挥了至关重要的作用。世界科学家联盟也把 ITU 当作一个组织性平台来使用，尽管是间接的使用。2001 年，联盟提出了一项“网络空间普遍条令”。其 2009 年 8 月的《网络稳定与网络和平埃利斯宣言》解释了网络和平的概念，进一步强调信息和观念的自由流动，解释了网络行为共同准则和全球立法框架的一体化，还解释了反网络犯罪的法律实施方面的努力，以及发展更具弹性的制度。最近，该联盟信息安全常设监测小组的主席、卸任的德国大使亨宁·维格纳尔，在 2011 年出版的《探索网络和平》一书中撰写了“网络和平”一章。[103]维格纳尔公开承认该行动是一次“通过转变角度以使网络战争非法化的努力”，与此同时“完全意识到数码基础设施目前广泛存在，而且将会不可避免地为恶意的、非和平的目的所利用”。[104]（参见乔治·莱考夫（George Lakoff）的书中关于框架化的重要性的讨论，他是加州大学伯克利分校的语言学教授。[105]）维格纳尔继续解释，“如果术语的使用更多地与政治或者政治中的重点问题紧密关联，并促使思想朝着正确选择的方向发展，那么自然会产生某种程度的开放式结局。定义不可以是封闭的，但其所列出的要素必须是相当直观并且是递进式的。”[106]

另一方面，ITU 的秘书长作为规范倡导者将世界科学家联盟也当作一个组织性的角色来利用。例如，《探寻网络和平》一书包括了 ITU 秘书长贡献的内容。[107]他提出的网络和平五项原则是：

“1. 所有政府都应致力于为其人民提供通讯渠道。

2. 所有政府都将致力于在网络空间保护其人民。

3. 所有国家都不应在其领土范围内庇护恐怖分子/罪犯。

4. 所有国家都不应首先向其他国家发起网络攻击。

5. 所有国家都必须在一项国际协作的框架内相互合作，以确保网络空间的和平。”[108]

[103] Wegener, 2011; World Federation of Scientists, 2003
[104] Wegener, 2011: 77
[105] Lakoff, 2006
[106] Wegener, 2011: 78
[107] Toure, 2011
[108] Wegener, 2011: 103

根据芬尼莫尔和斯金克的定义，一位规范倡导者注重以利他主义为动力，世界科学家联盟正符合这一经典定义。[109]该联盟的会员国在追求和平的过程中，看起来显然受利他主义的理想驱动。其1982年埃利斯宣言声称,“至关重要的是辨别出基础性要素,这对于启动一项有效进程来保护人类生活和文化避免某种第三方的、前所未有的灾难性战争是十分必要的。为了达到这一目的，有必要将单边行动的和平运动转变为真正的国际性行动,这种行动包含以互相真正的理解为基础的建议”。[110]

反恐执行工作队（简称CTITF）

反对以恐怖主义为目使用互联网工作组

反对以恐怖主义目使用互联网工作组可以被划作联合国网络安全工作组织网络的局外人。虽然它目前与联合国其他组织的活动相关，但是它的成立与大会关于网络安全的一般性讨论没有直接联系。它更像一个特殊案例，因为它起初是为回应9/11恐怖主义袭击而成立,在后来才与更广泛的网络安全辩论联系起来。

2011年9月28日，安理会通过第1373号决议成立了反恐怖主义委员会，以此作为对911袭击的回应。2004年，安理会通过第1535号决议设立了反恐怖主义委员会执行局，以监督第1373号决议的执行情况。该执行局目前由40位工作人员组成。[111]CTITF是由联合国秘书长于2005年创立的，目的是确保与第1373号决议相关的工作的协调，并于2009年归属政治事务部。[112]2006年，联合国《全球反恐战略》获得通过，这项战略中有这样一个段落，即探索“(a)在国际和地区层面达成合作性努力，以反对一切形式和表现的互联网恐怖主义；(b)以互联网作为工具反对恐怖主义的扩散，同时承认各国可以在这方面要求协助”的途径和方式。[113]

这就是CTITF其中一个工作组的基础，即“反对以恐怖主义目的使用互联网工作组”。2010年两位联合国的工作人员主要协助这个小组工作，一位的级别是主管官员，另一位的级别是青年专业官员。该小组有四个目标:(i)甄别并聚集以恐怖主义目的滥用互联网的利益攸关方和合作者,包括使用网络激进化、招聘、培训、运营策划、筹款和其他手段,(ii)发现恐怖主义使用互联网的方式,(iii)

[109]Finnemore and Sikkink, 1998: 898
[110]World Federation of Scientists “The Erice Statement”
[111] UN Counter-Terrorism Committee
[112] UN CTITF “Main Page”
[113] UN General AssemblyA/RES/60/288

定量审查该问题带来的威胁，并审查国家、地区和全球层面解决该问题的不同备选方案，（iv）审查联合国可能发挥的作用。[114]该小组由以下机构组成：

1267 委员会监测组
CTITF 办公室
文明联盟（于 2010 年某个时间点加入）
反恐执行局
公共信息部
国际刑事警察组织
人权事务高级专员办公室
反恐中人权促进和保护特别报告员
联合国教科文组织
联合国区域间犯罪与司法研究所
联合国毒品和犯罪问题办公室

2009 年 2 月，工作组根据 31 个会员国[115]提供的信息发布了一份初步报告，但工作组没有透露这 31 个国家的名称。工作组采用会员国使用的方法收集信息。报告主要的结论是“该领域目前还没有明显的恐怖主义威胁”，“尚不明确这是否是联合国反恐范围内的行动问题”。报告还建议“如果一种更加有形的恐怖主义袭击威胁确实在未来成为现实，那么更加合适和长远的解决方案是考虑使用一种新的国际反恐工具来对抗恐怖主义对重要基础设施的大范围袭击。我们要强调以恐怖主义目的使用互联网中存在的针对恐怖主义和针对互联网的差异性。而且，如果必要的话，可以更新重要基础设施的界定（或许通过条约议定书）以将信息基础设施包括进来，如果信息基础设施越来越重要的话。”报告也强调“反叙事

[114] UN CTITF “Working Groups”

[115] 阿富汗、阿尔及利亚、澳大利亚、奥地利、白俄罗斯、比利时、波斯尼亚和黑塞哥维那、加拿大、芬兰、德国、冰岛、日本、约旦、沙特阿拉伯、马耳他、摩洛哥，荷兰，新西兰，尼日利亚，挪威，阿曼，巴基斯坦，波兰，葡萄牙，俄罗斯，塞内加尔，塞尔维亚，西班牙，瑞士，英国和美国。

工作有令人振奋的承诺，但是仍处于萌芽期并需要进一步的解释”。[116]

关切类型	提到关切的国家数量
网络攻击 2	
筹款	4
培训	2
招募	6
机密	3
数据挖掘 3	
宣传共同关切	
激进化 1	

报告将以恐怖主义目的使用互联网的情况分为四种类型：

（i）实施恐怖主义袭击，其方式是远程改变计算机系统上的信息或者扰乱计算机系统之间的数据流动；

（ii）作为某种恐怖主义活动的信息资源；

（iii）作为散播与推进恐怖主义目标相关内容的手段；

（iv）作为向致力于追求或者支持恐怖主义行为的集体或者网络提供支持的手段。

报告归纳了成员国建议的联合国可以进一步有所作为的几种方式：

（i）促进成员国共享最佳解决措施；

（ii）建立一个研究以恐怖主义目的使用互联网的数据库；

（iii）为反极端主义意识形态做更多的工作；

（iv）建立国际法律措施，旨在限制恐怖主义内容在互联网上传播。

[116] UN CTITF, February 2009: 26

2011 年 5 月第二份报告发布，重点在于法律和技术方面的挑战。这份报告是在第一份报告的基础上完成的，并且是以 2010 年 1 月由德国外交部在柏林召开的一场会议，和 2010 年 2 月微软雷德蒙公司于华盛顿举办的一场会议为基础。报告中法律方面的内容强调目前已存在三种趋势：

（i）一些国家将目前网络犯罪的法律应用到互联网恐怖主义使用上；

（ii）一些国家将目前反恐法律应用到互联网相关的行为上；

（iii）一些国家已经针对互联网恐怖主义使用制定了具体法律。[117]

另外，报告还对针对互联网的法律和不针对互联网的法律进行了区分。例如，俄罗斯联邦 2006 年 7 月 27 日制定的关于信息、信息技术和信息保护的第 149-FZ 项法律第十条就不是针对互联网的。而另一方面，中国的《中国计算机网络和信息安全、保护和管理条令》第五条则是从法律的角度用一种针对互联网的方式来管理相关问题。

第二份报告还强调，9/11 袭击拓宽了对互联网可能如何被恐怖分子利用的理解。报告呼吁各国法律的一致化，方式是运用区域性法律文书，比如布达佩斯《网络犯罪公约》，或者英联邦《网络犯罪示范法》，以及国际性法律文书，比如《反跨国有组织犯罪条例》。报告中关于技术方面的内容更多的是关于技术上的可能性和以往技术滥用情况的概要。

工作组 2011 年起开始关注利用互联网进行反恐叙事，这包括 1 月份在沙特阿拉伯召开的一次大会。在此之后，第三份报告也开始撰写。[118]对于该问题的一项深入的研究有望于 2011 年下半年发布。[119]

II.2. 经济派别：网络犯罪

联合国关于犯罪的治理结构比典型的联合国系统还要复杂。因此，这里先进行一些解释性的说明。联合国大会、联合国会员国全体会议一直负责处理犯罪问题，同时处理犯罪问题的还有 ECOSOC，其会员国数量较少，由 193 个联合国会员国中的 54 个组成。除了 54 个会员国之外，ECOSOC 还有两个关注犯罪的功能委员会：麻醉药品委员会和预防犯罪和刑事司法委员会。两个委员会都是每年开

[117] UN CTITF, report May 2011: ix
[118] UN CTITF “Working Group on Countering the Use of the Internet for Terrorist Purposes”
[119] UN CTITF, May 2011: vii

一次会议。它们是 UNODC 这一联合国关注犯罪的官僚机构的管理部门。[120]最后，除了上述机构外，独立的联合国预防犯罪和刑事司法大会每五年召开一次会议。这个大会向预防犯罪和刑事司法委员会提出建议。我会首先分析联合国大会，之后对 ECOSOC 相关谈判进行解释，以此结束组织性平台 UNODC 的分析。

II.2.1. 大会第三委员会和 ECOSOC

关注“非法使用信息技术”的第三委员会[121]

在俄罗斯联邦向第一委员会提交决议的两年后，第三委员会——社会、人道主义和文化委员会——讨论了一份决议草案，题为“打击非法滥用信息技术”（A/55/59，2000 年 11 月 16 日），是犯罪预防和刑事司法工作的一部分。这份草案由美国和包括俄罗斯联邦、法国、以色列、英国在内的其他 38 个会员国提出，另还有 19 个会员国相继作为共同提案国。中华人民共和国不是共同提案国。[122]决议草案于 2001 年 1 月 22 日未经表决获得通过。

第 55/63 号决议的主要目的是建立一个“法律基础以打击非法使用信息技术”。[123]这项决议提到了于 1990 年设定的先例。那一年召开了联合国第八届预防犯罪和罪犯待遇大会并通过了一项关于计算机犯罪的决议。该决议还提到了欧洲委员会致力于布达佩斯《网络犯罪公约》所做的工作。决议的关键内容如下：

-“认识到**信息的自由流通**可以促进经济和社会发展教育以及民主施政[……]

-“表示对技术进步**为犯罪活动**尤其是为非法滥用信息技术**创造了新的机会**的关切[……]”

-“确认国家**与私营部门**必须合作打击非法滥用信息技术[……]”

-“打击非法滥用信息技术的斗争要求在制订解决办法时既考虑到保护个人自由和隐私也考虑到维护政府打击这种非法滥用的可能”[粗体为作者加注]。[124]

2001 年，美国和包括俄罗斯联邦、法国、以色列、韩国、英国在内的其他 73 个国家提出了一项后续决议，随后又有 8 个会员国作为提案国而加入。决议

[120]UNODC “Secretariat to the Governing Bodies Section”
[121] UN General Assembly A/RES/55/63
[122] UN General Assembly A/55/593
[123] UN General Assembly A/57/529/Add. 3
[124] UN General Assembly A/RES/55/63

草案于2002年1月23日未经表决而获通过。中华人民共和国不是此决议的共同提案国。[125]第56/121号决议概括了前面一项决议的目标，并将其表述为请“会员国在努力打击非法滥用信息技术时考虑到这些措施”。最终决议对决议草案进行了修改，序言中的第二自然段中将“民主与善治”改为“民主管治”。

更为重要的是，这项2002年的决议得出结论，委员会“决定推迟对本问题的审议，以待进行预防犯罪和刑事司法委员会打击与高技术和计算机相关的犯罪的行动计划中的预期工作”。[126]这一决定有效地将实质性的与网络犯罪有关的讨论从联合国大会转移到了预防犯罪和刑事司法委员会，该委员会是ECOSOC的功能委员会之一，也是UNODC的政府间机构之一，对此下文关于UNODC的章节将会作出解释。

接下来第三委员关于网络犯罪问题的唯一工作记录于大会第63/195号决议（2008），第64/179号决议（2009）和第65/232号（2011）决议中，题为“加强联合国预防犯罪和刑事司法方案，特别是其技术合作能力”。这些决议仅仅“提请注意[……]网络犯罪问题，并请联合国毒品和犯罪问题办公室在该办公室任务范围探讨处理这些问题的方式和方法”。[127]这些决议的前任，即第62/175号决议，其“盗用身份”的说法在第63/195号决议中首次得到了丰富，提到了“网络犯罪”这一术语。对这些决议的支持是由意大利领衔的。[128]这一系列决议的最新一项，即第65/232号决议不再使用“盗用身份”的说法，改为“赞赏地注意到召开了一次不限成员名额政府间专家组会议，全面研究网络犯罪问题”。[129]

关于第十二届联合国犯罪预防和刑事司法大会，联合国大会在第63/193号决议中将“犯罪分子使用科学技术方面以及主管机关利用科学技术打击犯罪包括网络犯罪方面的最新发展情况”批准为一项议程。[130]第65/230号决议要求将网络犯罪包括进UNODC的技术援助计划和能力建设。[131]

这使得第一委员会成为联合国大会迄今为止唯一一个实质上仍继续关注网络安全规范的委员会。

---

[125] UN General Assembly A/56/574

[126] UN General Assembly A/RES/56/121

[127] UN General Assembly A/RES/63/195; A/RES/64/179; A/RES/65/232

[128] UN General Assembly A/63/431; UN General Assembly A/64/440; UN General Assembly A/65/457

[129] UN General Assembly A/RES/65/232

[130] UN General Assembly A/RES/63/193; UN General Assembly A/63/431

[131] UNODC “Open-ended intergovernmental expert group”; UN General Assembly A/RES/65/230; UN ECOSOC E/2011/30

犯罪预防和刑事司法委员会

犯罪预防和刑事司法委员会的首次会议是在 1992 年。2010 年以前，网络犯罪一直都没有作为一个显著的主题出现在委员会的年度报告中。委员会 1994 年第三届会议的报告首次提到，他们正在考虑让第九届大会关注“计算机犯罪”技术合作方面的问题。[132]（这一早期活动的基础是 1990 年召开的第八届联合国犯罪预防与罪犯待遇大会及其关于计算机犯罪的决议。）1998 年，委员会最终请联合国大会将一场关于“计算机网络犯罪”的研讨会增加为第十届大会的一项议程。1999 年，委员会向 ECOSOC 提交了一份决议草案，是关于“联合国犯罪预防和刑事司法计划的工作”的，要求秘书长进行一项关于计算机犯罪的研究并在第十届大会上报告他的研究成果。这份草案还提到于 1998 年在日本举行的一次关于计算机网络犯罪的专家会议。但是，2000 年的报告并没有提及“网络”、“互联网”和“身份”等术语，但是却有一处提到“技术”，三处提到“计算机”。2001 年的报告情况类似。

2002 年的报告首次提到“网络”这个术语，而且使用了两次，同时还提到了《网络犯罪公约》。2003 年的报告又一次没有提到“网路”、“技术”和“身份”等术语。2002 年报告中“互联网”这个词被提到三次，“计算机”只在建议部分中被提到了一次，即建议第十一届大会期间召开一次“对抗高科技和计算机犯罪的措施”主题研讨会。2004 年的报告是首次有记载的呼吁出台一份对抗网络犯罪的《联合国公约》，并且提到是一位发言人向第十一届大会提出此建议。这份报告还包括向 ECOSOC 提交的第一份关于“通过国际合作预防、调查、起诉和惩罚诈骗、非法滥用和篡改身份等相关方面的犯罪”的决议草案（参见 ECOSOC 章节中的进一步分析）。2005 年和 2006 年的报告数次提到了上述术语，但是没有采取进一步的行动。2007 年的报告再次包括一份给 ECOSOC 的决议草案，即和 2004 年相同的关于“通过国际合作预防、调查、起诉和惩罚诈骗、非法滥用和篡改身份等相关方面的犯罪”的决议草案（参见 ECOSOC 章节中的进一步分析）。2008 年，委员会决定将“经济诈骗和与身份有关的犯罪”算作第十二届大会的两个讨论主题之一，并且作为一项议程，讨论“犯罪分子使用科学技术方面以及主管机关利用科学技术打击包括网络犯罪在内的不法行为的最新发展”。

[132] UN ECOSOC E/1994/31：65

2009 年，委员会举行了关于经济诈骗和与身份识别相关犯罪的主题讨论会，并准备了一份关于“通过国际合作预防、调查、起诉和惩罚诈骗、非法滥用和篡改身份等相关方面的犯罪”的决议草案供 ECOSOC 通过。该草案称《网络犯罪公约》是“目前唯一一项具体解决计算机诈骗、计算机伪造和其他形式的网络犯罪的条约。这些网络犯罪可能会为经济诈骗、与身份识别有关的犯罪、洗钱和其他相关的非法活动的实施提供帮助”（参见 ECOSOC 章节中的进一步分析）。委员会向 ECOSOC 提交的关于“犯罪预防和刑事司法委员会第十八届会议的报告，和第十九届会议临时议程与文件”草案决定，概述了委员会的决定，即“委员会第二十届会议的突出主题将是‘在数字时代保护儿童：儿童虐待和剥削方面的技术滥用’”。[133]

2010 年的报告提到，一些发言者再次提议出台一份全球性的打击网络犯罪的公约。该报告还包括委员会向 ECOSOC 提出的一项决议草案。联合国大会通过了这份决议草案，并要求委员会（这是一个循环过程）成立“一个不限成员名额的跨政府专家组，在委员会第二十届会议之前召集起来，对网上犯罪问题以及各会员国、国际社会和私营部门就此采取的对策进行一次全面研究，包括就国家立法、最佳做法、技术援助和国际合作开展信息交流，以期审查各种备选方案，加强现有和新的国家及国际打击网络犯罪的法律及相关对策”。[134]

截至目前，2011 年的报告是提到“网络”次数最多的一次报告。该报告中第 20/7 号决议题为“促进打击网络犯罪的相关活动，包括技术援助和能力建设”，引起了 ECOSOC 的注意。报告强调《反跨国有组织犯罪公约》可用于打击有组织犯罪中的网络犯罪。报告还向 ECOSOC 提出了一项决议草案，题为“利用新信息技术虐待和/或剥削儿童的预防、保护与国际合作”，并首次提到了网络欺凌。另一项关于“预防、调查、起诉和惩罚经济诈骗和身份相关犯罪的国际合作”的决议草案，要求 UNODC 继续就身份相关犯罪开展工作并积极使用政府间组织关于儿童问题研究的数据，建议专家组重视专家们关于身份识别相关犯罪的研究，并提到由加拿大政府自主编写的一份关于 UNODC 身份识别相关犯罪管治手册。

麻醉药品委员会的互联网与毒品贩运防治工作

麻醉药品委员会成立于犯罪预防和刑事司法委员会之前。它早在 1996 年第

[133] UN ECOSOC E/2009/30

[134] UN ECOSOC E/2010/30; UN ECOSOC resolution 2010/18; UN General Assembly A/RES/65/230

39 届会议上就已经关注互联网在毒品贩运犯罪方面的作用。[135]有趣的是，委员会较早的一份文件主要关注的是互联网在毒品控制方面的潜在积极作用。[136]1999 年，委员会的年会报告中有一个章节，内容是“沟通网络对毒品问题的影响，例如互联网”。[137]2000 年，委员会最终通过了一项决议，该决议仅关注“互联网”，并以“互联网”为标题，这引起了 ECOSOC 的注意。与较早的文件不同，这份决议强调万维网如何被用于或滥用于非法药物的推广和销售。美国和其他国家一同支持此项决议，但是俄罗斯和中国没有支持。[138]2000 年之后，没有任何一项关于互联网的具体决议出台，但是委员会的讨论中反复提到互联网。

2004 年，委员会提到 2000 年的决议，并为 ECOSOC 准备了一份决议草案。该草案获得通过并作为 ECOSOC 的第 2004/42 号决议，题为“通过互联网向个人销售国际管制合法药物”。[139]美国是草案的共同提案国，但俄罗斯和中国不是。2005 年，委员会通过了一项新的决议，这次决议的标题是“加强国际合作，以防止互联网被用于毒品相关的犯罪”。美国、俄罗斯和其他国家一道，都是此项决议共同提案国，但中国不是。该决议引起了 ECOSOC 的注意。[140]一项由美国作为共同提案国的类似决议于 2007 年获得通过，题为“通过国际合作防止通过互联网非法分销国际管制合法药物”，中国和俄罗斯都不是提案国。该决议提到第 43/8 号决议，也同样引起了 ECOSOC 的注意。[141]然而，麻醉药品委员会最后仅仅根据其功能权限，从一种毒品贩运的角度展开互联网方面的工作。

经济和社会委员会的身份识别相关犯罪防治工作

ECOSOC 于 2004 年首次通过了一项关于管治身份识别相关犯罪的决议。这一题为“通过国际合作预防、调查、起诉和惩罚诈骗、非法滥用和篡改身份信息等相关方面的犯罪”的第 2004/26 号决议的重点在于会员国，并且表达了对于“现代信息和沟通技术的广泛使用为诈骗、非法滥用与伪造身份带来广阔的新机会”的关切。[142]决议还要求秘书长召集成立一个政府间专家组，以准备一项关于诈骗和非法滥用与伪造身份的调查。专家组及其会议由加拿大和英国政府来支持。[143]

[135] UN ECOSOC E/1999/28/Rev.1: p .45
[136] UN General Assembly A/RES/S-20/4
[137] UN ECOSOC E/1999/28/Rev.1
[138] UN ECOSOC resolution 43/8 in E/2000/28
[139] UN ECOSOC E/2004/28
[140] UN ECOSOC resolution 48/5 in E/2005/28
[141] UN ECOSOC resolution 50/11 in E/2007/28/Rev. 1
[142] UN ECOSOC resolution 2004/26
[143] UN ECOSOC resolution 2009/22; UN ECOSOC E/CN.15/2009/2 and Corr.1

该决议的继任者，第2007/20号决议注意到“欧洲委员会的《网络犯罪公约》是一项国际性法律文书，不是欧洲委员会会员国的国家也可以批准或者加入此公约”，这就鼓励“会员国考虑同意”此公约。该决议还“要求联合国毒品和犯罪问题办公室根据要求和预算外资源的掌握情况，向会员国提供法律专业知识或其他形式的技术援助”。

这一系列决议的最后一项，第2009/22号决议，详细阐述了其对UNODC的要求并且提到了专家组的报告。该决议还声明：

“出于上面提到的原因，联合国《反跨国有组织犯罪公约》，联合国《反腐败公约》，以及一定条件下适用的欧洲委员会《网络犯罪公约》，以及13个反恐怖主义的普遍性法律文书等等，似乎都为相互法律援助、引渡和其他形式的国际合作提供了一个更完整的框架与法律基础，而这些合作对于处理跨国经济欺诈案件和与身份识别相关的犯罪是必需的。因此，政府间专家组认为在该领域不需要任何进一步的国际法律文书”，相反，专家组向会员国提出如果还未批准的话，需尽快批准这些文书。[144]

这项决议还概括了接下来专家组要做的工作：

“认可联合国毒品和犯罪问题办公室在建立联合国国际贸易法委员会并与之协商方面付出的努力。该委员会是与身份识别相关犯罪的核心专家组，并定期将来自各国政府、私营部门实体、国际和区域组织和学术界的代表召集在一起，以分享经验、制定战略，促进进一步研究并就对身份识别犯罪采取实际行动达成一致意见”。[145]

专家组已经建立起来，并举行了几次会谈。在第十二次联合国犯罪预防与刑事司法大会召开之前不久（2005年以来的首次会议），专家组发布了成果。正如前面提到的，大会议程中包括网络犯罪。然而，参加2010年4月在巴西萨尔瓦多举行的第十二次联合国犯罪预防与刑事司法大会的国家并没有就网络犯罪达成条约。[146]这场持续的辩论主要集中在这样一个问题，即起初由欧洲委员会通过的布达佩斯《网络犯罪公约》在得到信息社会世界首脑会议承认之后，是否将成为一项全球性公约，或者只是一项“区域性行动”。[147]

[144] UN ECOSOC E/CN.15/2007/8 and Add.1-3
[145] UN ECOSOC E/CN.15/2007/8 and Add.1-3
[146]Toure, 2011: 92
[147] UN ITU Global Strategic Report, 2008: 14

美国批准了条约，但是俄罗斯拒绝这样做。如本文前面提到的，只要条约允许由外国的法律执行机构进行跨境搜查，俄罗斯就会拒绝。相反，大会的成果文件请求犯罪预防与刑事司法委员会成立一个新的不限成员名额的政府间专家组：

“对**网上犯罪**问题以及各会员国、国际社会和私营部门就此采取的对策进行一次全面研究，包括就国家立法、最佳做法、技术援助和国际合作开展信息交流，以期审查各种备选方案，加强现有并提出新的国家和国际打击**网上犯罪**的法律和其他对策[粗体为作者加注]”。[148]

2011 年 1 月 17 日至 21 日，专家组在维也纳举行会议，来自 78 个会员国的代表参加了会议。会议报告中有一份研究主题和方法的清单，并提交给于 2011 年 4 月 11 日至 15 日在维也纳召开的委员会第十二届会议，这是第 65/230 号决议的第 11 个自然段中要求的内容。(参见 E/CN.15/2011/19 中研究主题和范围的清单)。联合国大在其第 65/232 号决议中“赞赏了召集的”专家组。[149]

II.2.2. 组织性平台：UNODC 和 UNICRI

联合国毒品和犯罪问题办公室

比起本文讨论的其他联合国组织，UNODC 的预算相对较多，但 UNODC 只有一位全职人员负责网络方面的工作。(这位工作人员之前在 UNICRI 工作）对 UNODC 的第一项要求是参与到技术援助中去，具体指的是始于 2008 年第三委员会和联合国大会第 63/195 号决议中提到的“网络犯罪”。作为回应，UNODC 于 2009 年 6 月负责法律执行的官员举行了一次关于网络犯罪的为期一周的研讨会。[150]另外，UNODC 预防恐怖主义部门已经就涉及到以恐怖主义目的使用互联网的案件向 CTITF 的一份出版物贡献了针对法律执行调查员和刑事司法官员的文章，并于 2012 年初发表。会员国第一次正式要求 UNODC 就以恐怖主义目的使用互联网开展工作是在 2011 年 4 月举行的犯罪预防与刑事司法委员会第二十届会议上[151]。而在前一年的第十九届会议上，就曾首次提到了这件事。[152]ITU 的网络法律工具和 UNODC 的工具模型类似，而且 ITU 的国家立法公共数据库是一项独特的法律分析资源。

[148] UN General Assembly A/CONF.213/18
[149] UN General Assembly A/RES/65/232
[150]UNODC “Law enforcement officers trained”
[151] UN ECOSOC E/2011/30
[152] UN ECOSOC E/2010/30

联合国区域间犯罪和司法研究所（UNICRI）

设在意大利都灵的 UNICRI 是联合国系统中若干较小的机构之一。该研究所研究的重点和范围是在犯罪预防和刑事司法领域,协助政府间组织、政府类组织、和非政府组织制定和实施优化的政策。它与德国的马克思·普朗克研究所和瑞士的巴塞尔治理研究所共同出版杂志《F3——免于恐惧（Freedom From Fear)》。它最新一期杂志，也就是第 7 期，关注的是网络安全。

从网络安全的角度看，UNICRI 的特殊力量在于，拉乌尔·基耶萨（Raoul Chiesa）这位拥有技术专长的前黑客，以顾问的身份无偿支持这个研究所。他是黑客画像项目的领袖。2008 年，该项目的成员出版了一本题为《黑客画像——罪犯画像科学在黑客世界中的应用》的书。这个项目令人瞩目的贡献之一是它试图将一种行动者分类技术用于网络空间。他们识别出了“疯狂的拉默”、“脚本小子”、“37337 K-rAdiRC #黑客零日攻击者”、“破解者”、“道德黑客”、“安静、偏执、娴熟的黑客”、“工业间谍”、“网络战士”、“政府代理”、“军事黑客”（均为黑客程序的名称，——译者注)。[153]因为这些黑客类型有时是重叠的，可以将它们简化为网络战争中的三类组织:

数码战士:私人行动者,技术高超的佣兵,为了钱财和理想而进行黑客攻击,有罪犯也有恐怖分子。

政府代理:“公民国家行动者”——受雇于一个国家的平民政府的黑客，他们为（打击）间谍、政府信息监测、恐怖主义组织、战略产业，和未经授权而通过使用电子世界来造成现实伤亡的个人。[154]

军事黑客:“军事国家行动者”——受雇于一个国家军队的黑客，他们潜在地得到授权，并在战争情况下利用电子世界造成现实中的伤亡。

这种分类在克拉克和康科的研究中有更详细的阐述。他们仅仅将网络战士这个词的通常用法分为罪犯和军事黑客两种。UNICRI 的分类可以更加清晰地区分网络战争中不同的行动者,比如国家与非国家的行动者,以及军事与民用行动者。（UNICRI《黑客画像——罪犯画像科学在黑客世界中的应用》一书也有一篇不同黑客攻击技术的概要。[155]）这是特别有价值的贡献，因为活动于网络空间的不同

[153]Chiesa et al, 2009: 52-56, 61
[154]Chiesa et al, 2009: 56
[155]Chiesa et al, 2009: 20-32

行动者在媒体以及某些学术文献中通常没有被正确地分类。混淆参与丑化网络的青少年和震网的发明者，并且将二者放在一起考虑，这只会使其看起来像是个骗局。[156]

2010 年，UNICRI 致力于为 ITU 的儿童在线保护行动制定一系列方针。[157]

II.3.大会第二委员会——“全球网络安全文化”

大会第二委员会关于“全球网络安全文化”的三项决议将两个派别——政治-军事派和经济派——联系了起来，分别指向第一和第三两个委员会的决议。[158]

第三委员会决定不再关注网络犯罪，在此之后，美国于 2002 年提出了一项新的决议草案,这一次美国是向第二委员会提出的——也就是经济和财政委员会——草案题为“创造全球网络安全文化”。这项草案是“宏观经济政策问题：科学和技术的发展”这场持续辩论的一部分。[159]草案的提出也代表日本的想法，澳大利亚和挪威也加入到最初草案共同提案国的行列中。经过几次修改之后，包括俄罗斯联邦、法国、韩国在内的另外 36 个会员国也成为决议草案的共同提案国。草案经过修改之后，最终的决议文本（A/RES/57/239）也提到了第一委员会所通过的决议。该草案未经投票而获通过。中华人民共和国不是此项决议的共同提案国。[160]（很不幸，在决议通过之后，美国和另外四个会员国的代表的陈述没有被编号为 A/C.2/57/SR.44 的文件提到，而这份文件在第二委员会第 A/57/529/Add.3 项报告中被引用）。对最初的草案所做的三处重要修改是：

-第一，增加了一个自然段，注意到“各国在获得和利用信息技术方面的差距会削减国际合作打击非法滥用信息技术和创造全球网络安全文化的成效”。这一自然段关键的论点是发展中国家对于“信息技术的转让，尤其是向发展中国家转让”的众所周知的定期呼吁。这一点，以及能力建设的需要，都在这份决议中最后一个操作性段落中得到了重申，而且这很可能是会员国谈判后妥协的结果，以换取发展中国家同意通过此项决议草案。这个句子当中的明显矛盾之处——如果在获得信息技术上有差距,那么那些差距也会影响到非法滥用,对此有解释是，不同国家在获取技术上或许是有差距的，但那些国家的罪犯却不一定有此差距。

[156] Singer, 2011
[157] UNICRI “Cybercrimes”
[158] UN General Assembly A/RES/57/239; A/RES/58/199; A/RES/64/211
[159] UN General Assembly A/57/529/Add. 3
[160] UN General Assembly A/57/529/Add. 3

-第二，将最初的措辞“通过本决议附件所列的原则”改为“注意到本决议附件所列的要点”，这意味着原本的语言被削弱了，因为将“原则”一词改为了弱一些的“要点”，而通常术语学的排列顺序依次是“通过”/“欣见”/“赞赏地注意到”/“注意到”/“承认”。根据这些“要点”，某种全球网络安全文化可以说是要求九个互补性的要点：意识、责任、反应、道德、民主、风险评估、安全设计和实施、安全管理和再行评估（参见附录）。虽然措辞有所变化，但是这些要点可以被视为就基本国际原则形成共识的首次尝试和规范出现的信号。

-第三，最后的决议仅仅“邀请”而不是“要求”会员国注重该决议，因为2005 年在突尼斯举办的信息社会世界首脑会议有来自私人部门和公民社会的代表。这次突尼斯首脑会议聚集的参与者有1500 名来自国际组织，6200 名来自非政府组织，4800 名来自私营部门，和970 名来自媒体的代表。

全球网络安全文化的第二份决议于2004 年开始谈判，并于2005 年1 月在联合国大会上获得通过。这份决议的内容有所丰富，将保护重要信息基础设施囊括了进去，并在附件中提炼出了关键的要点（参见附录）。这些要点的基础是2003 年召开的八国集团司法部长和内政部长会议。这种关联又是一个信号，说明在国际上受到各个国家认可的各种要点和原则，是如何开始形成一个网络，而这一网络有可能发展成为一项制度。[161]有趣的是，这项决议不再谈及政府对新技术的依赖，取而代之的是国家重要基础设施和国家重要信息基础设施之间的联系。包括中国在内的总共 69 个国家是这项决议的共同提案国，但俄罗斯不是。[162]与第一份草案相比，最终的文本（第58/199 号决议）的序言中增加了一个新的自然段，讲的是“每一个国家都将确定自己的重要信息基础设施”。最终的文本还新增加了操作性内容，鼓励会员国分享最佳做法。

第三份决议，也就是第64/211 号决议，在美国政策发生转向之后于2010 年获得通过。此项决议第二部分的题目“创建全球网络安全文化以及评估各国保护重要信息基础设施的努力”揭示了这份文件的部分重要内容。该决议有一份附件（参见附录），概括出一项“国家保护重要信息基础设施努力自愿自我评估工具”，为会员国提供了一幅详细的路线图。此项决议由美国代表另外39 个国家提出。俄罗斯和中国不是该决议的提案国。对最初的草案做的关键修改是：

-第一，最初决议草案文本中公民社会和商业的提法不再保留。提及“表达

[161] UN ITU Global Strategic Report, 2008: 24
[162] UN General Assembly A/58/481/Add.2

自由和信息、观念与知识自由流动”的章节也删掉了。一同删掉的还有以第六十五届大会为设定期限提交相关信息的建议。

-第二，最终的文本强调“互联网治理论坛必须承担讨论各种问题的任务”和“重申各国政府在国际互联网治理方面应该平等发挥作用和承担责任”，这些关系到更大范围的互联网治理辩论。文本还强调“每一个国家都将自行决定本国的重要信息基础设施”。

-第三，决议强调“通过国际信息分享和协作支持各国的努力，以便有效应对这些越来越具有跨国性质的威胁”,并鼓励成员国共享最佳实践方法以供传播。

附件中只对语言做了细微的编辑。

Ⅲ. 互联网治理论坛

成立互联网治理论坛的依据是突尼斯议程的第 72 个自然段，也就是 2005 年 11 月 16 日至 18 日召开的第二阶段信息社会世界首脑会议的成果文件。成员国就联合国和网络问题作出了两项重要的决定。第一，成员国要求联合国秘书长成立 IGF，这也是本节所关注的内容。[163]第二，如前面所讨论的，ITU 被授权负责 C5 行动方针，即“建立使用 ICT 的信心和安全”。[164]（另一方面，首脑会议的成果文件重申了联合国大会关于网络安全文化的第 57/239 号决议，但是没有提及重要信息基础设施的保护，尽管大会第 A/RES/58/199 号决议中有此请求。但是成果文件也的确提到了关于信息技术非法滥用的决议。[165]）

在 2005 年信息社会世界首脑会议上也发生了一场争论。[166]这场各国政府间的争论是关于域名治理的。目前域名治理由 ICANN 负责。ICANN 由美国人牢牢地把控着，一直被那些想要拥有发言权的政府警觉地监视着。例如，2010 年中国政府在其互联网政策白皮书中写道“中国认为，联合国在国际互联网管理中发挥的作用应该是全方位的”。[167]在突尼斯，一些欧盟会员国支持推动成立一个政府间组织以取代 ICANN。美国最终妥协了，IGF 作为一个论坛成立起来。在这个论坛上，“各国政府可以进行辩论，并就互联网政策问题提出建议，但不行使直接的政策权威”。在突尼斯做出的妥协是为寻求控制互联网命名系统所进行的争吵的

[163] UN World Summit on the Information Society, 2005: 17
[164] UN World Summit on the Information Society, 2005: 26
[165] UN World Summit on the Information Society, 2005: 13
[166] Wu and Goldsmith, 2008: 171
[167] Ford, 2010: 65

最后一轮——也是一场寻求控制互联网的更大规模的战争。现在说谁赢得了这场战争的胜利都为时过早。[168]（参见斯特兰（Zittrain）关于 IGF 和域名治理的重要分析，第 242-243 页，以及吴（Wu）和戈德史密斯（Goldsmith）在 2008 年关于这场辩论早期阶段的研究，第 41-42 页。）

IGF 一直以来依靠自愿捐助，其首脑向联合国主管经济和社会事务部的副秘书长汇报工作，目前担任首脑的是来自中国的沙祖康（ShaZukang）。IGF 的工作人员有执行协调员[2006 年至 2011 年是马库斯·库默尔（Markus Kummer）[169]]，一名项目和技术经理，和两名兼职顾问。[170]IGF 将建议提交给联合国秘书长，而秘书长转而又将这些建议提交给联合国大会。[关于 IGF 未来发展的评估可参见基伦·麦卡锡（Kieren McCarthy）的研究。[171]]

结论

联合国的活动清晰地显示出新的网络规范正在慢慢出现。支持这一论点的关键证据是，随着时间的推移，特别是在 2005 年以后，联合国大会各委员会通过的决议数量，附件中的要点，数量不断上升的共同提案国，以及对于各官僚结构介入到该问题（指规范出现，——译者注）之中的要求和提供技术援助的要求。而且，一个新的政府专家组将于 2012 年成立，并于 2013 年提交报告，这标志着政治-军事派别和规范出现过程进入下一个阶段。

然而，我对两个派别的分析也显示出规范出现的过程是动态的。我概括了每一个派别的谈判是如何与另一个派别发生关联,谈判以之前的发展成果为基础并强化了之前的发展。我指出在国际层面一个规范生命周期的动力是如何依赖于(i)不断变化的行动者之间的整体关系,而这一整体关系受包括政府更迭在内的某些国内条件的影响也不断发生变化。(ii）外在因素，这些外在因素改变了资深政策制定者的观念，比如那些在 2007 年占据头条的网络事件。

俄罗斯在这一过程中一直扮演着至关重要的角色，而美国则是最重要的制衡力量。德国、加拿大和英国也发挥了积极作用，这些国家资助了各种研究项目和专家组织。有趣的是，中国看起来相当被动，唯一一次例外是中国支持第一委员会的一项决议,这发生在美国第一次决定投票反对此项决议和最近的行为准则的

[168] Wu and Goldsmith, 2008: 171
[169]UN Internet Governance Forum “Past Staff Members”
[170]UN Internet Governance Forum “About IGF”
[171] McCarthy, 2011

一年后。

本文证明了国家作为规范倡导者的重要作用。虽然国家的动机可能主要受本国利益以及某种结果逻辑的驱动,但是结果逻辑并不一定排除利他主义的动机和某种具有影响力的适当性逻辑。正如彼得·A·豪尔（Peter A. Hall）和罗斯玛丽·C. R·泰勒（Rosemary C.R. Taylor）两位学者指出，二者并不互斥。[172]阅读俄罗斯政府官员所发表的观点会发现这一点暗含其中。例如，科莫夫、罗特科夫和戴莱夫斯基，还有斯特雷索夫多次提到联合国宪章，并以道德论点来证实其推理脉络。[173]

联合国系统本身的网络安全工作是相当碎片化的。每一个组织被会员国作为组织性平台用来推进它们自己的议程。然而，各个组织也做了一些重要的工作。例如，以恐怖主义目的使用互联网工作组发表的报告，揭示了一些有意思但是罕见的数据，这些数据是关于各个国家对于网络安全威胁的看法（虽然事实是报告没有具体指明哪些信息是由哪个国家提交的）。从组织理论的角度继续前进，问题就变成了如何最有效地利用专长和各种行动的努力,与此同时尽量避免过去的陷阱并潜在地采用更多类似网络的结构,因为各个组织工作人员人数不多而且有地域差异。

我们甚至还可以发现一些没有预料到的结果。ITU 给予网络和平行动的积极支持，有可能超越 ITU 的委托人（也就是其会员国）本来的意图，该行动是由世界科学家联盟推动的。这发生在突尼斯首脑会议上，当时委托人派给 ITU 掌管 C5 行动方针的任务。毕竟世界科学家联盟的原则中有这样一种诉求，即“所有政府都应该尽力减少或者消除信息、观念和人口之间自由流动的限制。这样的限制会增加世界上的怀疑和敌意”，这一诉求写在其 1982 年埃利斯声明中。这将使俄罗斯政府之前的努力付诸东流，也就是福特所强调的，俄罗斯利用互联网控制信息流动的努力。

至于未来研究的步骤和问题，以下四个主题仅仅是研究清单的开始，不能穷尽所有问题：

第一，鉴于第一委员会的工作，几个会员国向联合国秘书长提交了不同的声明。在这些声明中，它们概述了其关于网络安全的立场和观点。这看起来是很丰

[172] Hall and Taylor, 1996
[173] Komov et al, 2007; Streltsov, 2007

富的信息，可以用于描绘一幅更加全面的图景，即关于全球范围内不同国家如何思考网络安全这一问题，以及它们的想法如何随着时间推移而发生变化的图景。美国的政策转向是一种战术行动还是一种具有长期后果的战略行动？更宽泛地说，复杂的权力结构问题也出现了。例如，美国国务院是美国政府在国际组织中的官方代表。那么，国防部或者商务部在处理网络安全问题时是否应该和国务院坐在一起？克里斯·佩特（Chris Painter）担任国务院网络问题协调员这一新职务，他的作用是什么？又例如俄罗斯外交部和国防部如何协调它们在 ITU 中的位置？那么中国政府又该如何做呢？

第二，未来对于每一个联合国下属机构的深度分析可以丰富本文有限的、有时仅仅是描述性的解释。尤为值得注意的是一些传闻，这些传闻暗示了某些国家利用某些联合国组织作为组织性平台。例如，有这样一种言论，即 UNODC 是一个受“美国人”影响的组织，而 ITU 则处于“俄罗斯和中国”的影响之下。这样的言论可能指的是组织首脑的国籍，或者组织首脑受教育的地点，也可能指的是组织的主要资金来源。例如，ITU 现任秘书长，哈玛德·图埃是在俄罗斯接受的大学教育[174]，也或者以主要的投资人作为指标。这种观点值得进一步探究，以便清楚地了解一个组织究竟如何被一位规范倡导者利用，或者同时被不同的规范倡导者利用。

第三，联合国是多边主义世界唯一的参与者。一个显而易见的问题是，联合国在纽约、日内瓦和都灵的活动如何与欧盟的活动，以及布鲁塞尔的北大西洋公约组织、巴黎的经济合作与发展组织，或者是雅加达的东盟的活动联系起来。类似地，三个联合国大会委员会的互动如何相互影响。我的分析已经强调了这些联系中的两点，即八国集团通过的原则和以欧洲委员会为基础的布达佩斯《网络犯罪公约》。

第四，过去十年中出现了规范出现的第一批信号，那么接下来会出现规范扩散吗？这一过程是动态的，那么什么时候以及基于什么原因才会出现起起伏伏？我的分析已经指出了一个明显的原因，即会员国的国内政治环境和政府更迭。然而，这也可以仅被理解为某些更大趋势的征兆。影响规范起起落落的其他因素有哪些？又是在哪些条件下发生影响？外部的规范倡导者，比如世界科学家联盟，是如何恰好影响了这一过程，它们是否可能继续这样做并且其他人由于意识愈发深刻也加入其中？而且，正在浮现的规范是否会受到既存规范体系的溢出效应的

[174]Toure, 2011: viii-ix

影响，或者它们完全是新的规范？这些既存规范与犯罪和军事活动有关，而这些活动可以经过调整之后应用到网络空间中去。

简言之，关于网络安全和国际关系的研究仍然处于初级阶段。每一篇新文章都可能提出而不是回答更多的问题。当俄罗斯于 1998 年提出第一份决议草案时，很多辩论还停留在科幻小说的范畴，但是震网事件发出了信号，即小说变成了科学。在首次尝试对网络安全进行定义的十余年之后，仍未就此形成正式共识。但是，过去十年的活动显示了相较于典型国际关系时间轴，规范在网络空间出现的的速度是惊人的。

[蒂姆·毛瑞尔(Tim Maurer):美国哈佛大学肯尼迪学院;曲甜：清华大学政治学系；王艳:中央编译局。]

參考文献

Abbott, Kenneth W., and Duncan Snidal. “Hard and Soft Law in International Governance.” *International Organization* 54.3 (2000): 422.

Barnett, Michael N., and Liv Coleman. "Designing Police: Interpol, and the Study of Change in International Organizations." *International Studies Quarterly* 49 (2005): 593-619.

Barnett, Michael and Martha Finnemore. “Rules for the World – International Organizations”.in *Global Politics*. New York: Cornell University Press, 2004.

Barnett, Michael and Martha Finnemore. "The Politics, Power, and Pathologies of International Organizations." *International Organization* 53.4 (1999): 699-732.

Boyle, Alan E. “Some Reflections on the Relationship of Treaties and Soft Law.” *The International and Comparative Law Quarterly* 48.4 (1999): 901-02.

Broad, William J., John Markoff and David E. Sanger. “Israeli Test on Warm Called Crucial in Iran Nuclear Delay”. *The New York Times*. 15 January 2011.

Carr, John. “Online Crimes against Children”.*F3 Freedom from Fear 7* (2010). Last accessed 12 October 2011. <http://www.freedomfromfearmagazine.org/index.php?option=com_content&view=article&id=308:online-crimes-against-children-&catid=50:issue-7&Itemid=187>

Chiesa, Raoul. *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*. UNICRI: Turin, 2008.

Chinkin, C. M. “The Challenge of Soft Law: Development and Change in International Law.” *The International and Comparative Law Quarterly* 38.4 (1989): 850-66.

Clarke, Richard A. and Robert Knake. *Cyber War: The Next Threat to National Security and What To Do About It.*Ecco, April 2010.

Deibert, Ronald. “Ronald Deibert: Tracking the emerging arms race in cyberspace”. *Bulletin of the Atomic Scientists 67.1 (January/February 2011). Last accessed 12 October 2011.* <http://bos.sagepub.com/content/67/1/1.abstract>

Eriksson, Johan and GiampieroGiacomello. “The Information Revolution, Security, and International Relations: (IR)relevant Theory?” *International Political Science Review* 27.3 (2006): 221-244.

Finnemore, Martha, and Kathryn Sikkink. "International Norm Dynamics and Political Change." *International Organization 52.4* (1998): 894-905.

Ford, Christopher A. “The Trouble with Cyber Arms Control”.*The New Atlantis – A Journal of Technology & Society*. (Fall 2010): 52-67.

Geers, Kenneth. “Cyber Weapons Convention”. Computer Law and Security Review 23 (2010): 547-551

Gorman, Siobhan. “U.S. Backs Talks on Cyber Warfare”.*The Wall Street Journal* (4 June 2010). Last accessed 12 October 2011. <http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html>

Hall and Taylor. “Political Science and the Three New Institutionalisms”. *Political Studies* XLIV (1996): 955-956

Hillgenberg, Hartmut. “A Fresh Look at Soft Law”.*European Journal of International Law* 10.3 (1999): 499-515.

Kingdon, John W. Agenda, *Alternatives, and Public Policies.* New York: Longman, 2003.

Komov, Sergei, Sergei Korotkov and Igor Dylevski. “Military aspects of ensuring internaitonal information security in the context of elaborating universally acknowledged principles of internaitonal law”. *Disarmament Forum* 3 (2007) Last accessed 12 October 2011. <http://www.unidir.org/pdf/articles/pdf-art2645.pdf>

Krasner, Stephen. *International Regimes.* Ithaca, NY: Cornell University Press, 1983: 2

Lakoff, George. *Thinking Points: Communicating our American Values and Visions*. Farrar, Straus, and Giroux: 2006.

Lessig, Lawrence. “The regulation of social meaning”.*The University of Chicago Law Review* 62.3 (1995): 944-1045.

March, James G., and Johan P. Olsen. "The Institutional Dynamics of International Political Orders." *International Organization* 52.4 (1998): 943-69.

Markoff, John and Andrew E. Kramer. “In Shift, U.S. Talks to Russia on Internet Security”.*The New York Times.* 13 December 2009.

Markoff, John. “Step Taken to End Impasse Over Cybersecurity Talks”.*The New York Times*. 16 July 2010.

McCarthy, Kieren. “Global Internet governance fight looms”. .*nxt blog* (22 September 2011). Last accessed 12 October 2011. <http://news.dot-nxt.com/2011/09/22/internet-governance-fight-looms>

Nakashima, Ellen. “15 nations agree to start working together to reduce cyberwarfare threat”.*The Washington Post.*17 July 2010.

Nazli, Choucri. “Introduction: CyberPolitics in International Relations” *International Political Science Review* 21.3 (2000): 243-263.

Nye Jr, Joseph S. “Nuclear Lessons for Cyber Security?” *Strategic Studies Quarterly* (forthcoming 2011)

Nye Jr, Joseph S. “Cyberpower”.*Paper.* Cambridge, Mass.: Harvard Belfer Center for Science and International Affairs, May 2010.

Pradesh, Andhra. “ITU mullying ‗cyber treaty‘ to curb cyber crime” *The Hindu* (25 May 2011). Last accessed 12 October 2011. <http://www.hindu.com/2010/05/25/stories/2010052562310800.htm>

Russian Federation.*Convention on International Information Security*

(Concept).Ekaterinburg, Russia: International Meeting of High-Ranking Officials Responsible for Security Matters, 21-22 September 2011.

Schwartau, Winn. "Testimony before Congress" (27 June 1991). Last accessed 12 October 2011. <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA344848>

Segal, Adam. "China and Information vs. Cyber Security" Council on Foreign Relations blog (15 September 2011). Last accessed 3 October 2011. <http://blogs.cfr.org/asia/2011/09/15/china-and-information-vs-cybersecurity/>

Singer, Peter W. "The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity is Misplaced and Counterproductive". Brookings Government Executive. Last accessed 12 October 2011. <http://www.brookings.edu/articles/2011/0815_cybersecurity_singer_shachtman.aspx>

Streltsov, A.A. "International information security: description and legal aspects". *Disarmament Forum* 3 (2007) Last accessed 12 October 2011. <http://www.unidir.org/pdf/articles/pdf-art2642.pdf>

The Hindu Business Line. "Cyber war: Take no-first-attack vow, ITU tells nations" (24 May 2010). Last accessed 12 October 2011. <http://www.thehindubusinessline.in/bline/2010/05/25/stories/2010052552450700.htm>

Toure, Hamadoun I. "Cyberspace and the Threat of Cyberwar", in The Quest for Cyber Peace. International Telecommunication Union and World Federation of Scientists, January 2011.

Toure, Hamadoun I. "ITU's Global Cybersecurity Agenda", in *The Quest for Cyber Peace*. International Telecommunication Union and World Federation of Scientists, January 2011.

Toure, Hamadoun I. "The International Response to Cyberwar", in *The Quest for Cyber Peace*. International Telecommunication Union and World Federation of

Scientists, January 2011.

United Nations. Counter-Terrorism Implementation Task Force. “CTITF Working Group Compendium – Countering the Use of the Internet for Terrorist Purposes – Legal and Technical Aspects”. *CTITF Publication Series*. New York: United Nations, May 2011.

United Nations. Counter-Terrorism Implementation Task Force.“Main Page”. Last accessed 3 August 2010. <www.un.org/terrorism/cttaskforce.shtml>

United Nations. Counter-Terrorism Implementation Task Force.*Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes.*New York: United Nations, February 2009.

United Nations. Counter-Terrorism Implementation Task Force.“Working Groups”. Last accessed 3 August 2010.
< https://www.un.org/terrorism/workinggroups.shtml>

United Nations. Counter-Terrorism Implementation Task Force. “Working Group on Countering the Use of the Internet for Terrorist Purposes”. Last accessed 12 October 2011. <http://www.un.org/terrorism/internet>

United Nations. Economic and Social Council.*2010 ECOSOC General segment briefing on ‘Cyber security: emerging threats and challenges’ Friday, 16 July, 3:00-4:30 p.m. Background Note.* Last accessed 12 October 2011. <https://www.un.org/en/ecosoc/julyhls/pdf10/gs_briefing_background_note.pdf >

United Nations. Economic and Social Council.*2010 ECOSOC General segment briefing on ‘Cyber security: emerging threats and challenges’ Friday, 16 July, 3:00-4:30 p.m. Statements. Last accessed 12 October 2011.* <https://www.un.org/en/ecosoc/julyhls/pdf10/cyber_security_statement.pdf>

United Nations. Economic and Social Council.*Commission on Crime Prevention and Criminal Justice: Report of the Secretary-General – International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.* E/CN.15/2009/2. New York: United Nations, 3 February

2009.

United Nations. Economic and Social Council.*Commission on Crime Prevention and Criminal Justice: Report of the Secretary-General – Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity.* E/CN.15/2007/8*. New York: United Nations, 2 April 2007.

United Nations. Economic and Social Council.*Commission on Crime Prevention and Criminal Justice – Report on the twentieth session.*E/2011/30*. New York: United Nations, 2011.

United Nations. *Economic and Social Council. Commission on Crime Prevention and Criminal Justice – Report on the nineteenth session.* E/2010/30. New York: United Nations, 2010.

United Nations. Economic and Social Council.*Commission on Crime Prevention and Criminal Justice – Report on the third session.* E/19940/31. New York: United Nations, 1994.

United Nations. Economic and Social Council.*Commission on Narcotic Drugs – Report on the fiftieth session: Resolution 50/11.* E/2007/28/Rev.1. New York: United Nations, 2007.

United Nations. Economic and Social Council.*Commission on Narcotic Drugs – Report on the forty- eighth session: Resolution 48/5.* E/2005/28. New York: United Nations, 30 March 2005.

United Nations. Economic and Social Council.*Commission on Narcotic Drugs – Report on the forty- seventh session.*E/2004/28. New York: United Nations, 2004.

United Nations. Economic and Social Council.*Commission on Narcotic Drugs – Report on the forty-third session: Resolution 43/8.* E/2000/28. New York: United Nations, 2000.

United Nations. Economic and Social Council.*Commission on Narcotic Drugs –*

*Report on the forty- second session.*E/1999/28/Rev.1. New York: United Nations, 1999.

United Nations. *Economic and Social Council.Resolution 2010/18 – Twelfth United Nations Congress on Crime Prevention and Criminal Justice.*E/2010/18. New York: United Nations, 22 July 2010.

United Nations. *Economic and Social Council.Resolution 2009/22 – International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity related-crime.* E/2010/18. New York: United Nations, 30 July 2009.

United Nations. *Economic and Social Council.Resolution 2004/26 – International cooperation in the prevention, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.*E/2004/26. New York: United Nations, 21 July 2004.

United Nations. General Assembly. *First Committee draft resolution - Developments in the field of information and telecommunications in the context of international security.*A/C.1/61/L.35. New York: United Nations, 11 October 2006.

United Nations. General Assembly. *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.* A/66/359. New York: United Nations, 14 September 2011.

United Nations. General Assembly. *Note by the Secretary-General 65/201 - Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* A/65/201. New York: United Nations, 30 July 2010.

United Nations. General Assembly. *Report of the First Committee 65/405 - Developments in the field of information and telecommunications in the context of international security.*A/65/405. New York: United Nations, 9 November 2010.

United Nations. General Assembly. *Report of the First Committee 61/389 -*

Developments in the field of information and telecommunications in the context of international security. A/61/389. New York: United Nations, 9 November 2006.

United Nations. General Assembly. *Report of the First Committee 60/452 - Developments in the field of information and telecommunications in the context of international security.* A/60/452. New York: United Nations, 16 November 2005.

United Nations. General Assembly. *Report of the Second Committee 64/422/Add. 3 – Globalization and Interdependence: science and technology for development.* A/64/422/Add.3. New York: United Nations, 15 December 2009.

United Nations. General Assembly. *Report of the Second Committee 58/481/Add. 2 - Macroeconomic policy questions: science and technology for development.* A/58/481/Add.2. New York: United Nations, 15 December 2003.

United Nations. General Assembly. *Report of the Second Committee 57/529/Add. 3 - Macroeconomic policy questions: science and technology for development.* A/57/529/Add.3. New York: United Nations, 12 December 2002.

United Nations. General Assembly. *Report of the Secretary-General 60/202 - Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* A/60/202. New York: United Nations, 5 August 2005.

United Nations. General Assembly. *Report of the Third Committee 65/457 - Crime prevention and criminal justice.*A/65/457. New York: United Nations, 6 December 2010.

United Nations. General Assembly. *Report of the Third Committee 64/440 - Crime prevention and criminal justice.*A/64/440. New York: United Nations, 1 December 2009.

United Nations. General Assembly. *Report of the Third Committee 63/431 - Crime prevention and criminal justice.*A/63/431. New York: United Nations, 4 December 2008.

United Nations. General Assembly. *Report of the Third Committee 56/574 - Crime prevention and criminal justice.*A/56/574. New York: United Nations, 7 December 2001.

United Nations. General Assembly.*Report of the Third Committee/55/593 - Crime prevention and criminal justice.* A/55/593. New York: United Nations, 16 November 2000.

United Nations. General Assembly. *Report of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice.* A/CONF.213/18. Salvador, Brazil: United Nations, 18 May 2010.

United Nations. General Assembly. *Resolution 65/232 - Strengthening the United Nations crime prevention and criminal justice programme, in particular its technical cooperation capacity.* A/RES/65/232. New York: United Nations, 23 March 2011.

United Nations. General Assembly. *Resolution 65/230 - Twelfth United Nations Congress on Crime Prevention and Criminal Justice.*A/RES/65/230. New York: United Nations, 1 April 2011.

United Nations. General Assembly. *Resolution 64/211 - Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures.* A/RES/64/211. New York: United Nations, 17 March 2011.

United Nations. General Assembly. *Resolution 63/193 – Preparations for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice.* A/RES/63/193. New York: United Nations, 24 February 2009.

United Nations. General Assembly. *Resolution 60/288 – The United Nations Global Counter-Terrorism Strategy.*A/RES/60/288. New York: United Nations, 20 September 2006.

United Nations. General Assembly. *Resolution 57/239 - Creation of a global culture of cybersecurity.* A/RES/57/239. New York: United Nations, 31 January 2003.

United Nations. General Assembly. *Resolution 56/121 - Combating the criminal misuse of information technologies.* A/RES/56/121. New York: United Nations, 23 January 2002.

United Nations. General Assembly. *Resolution 55/63 - Combating the criminal misuse of information technologies.* A/RES/55/63. New York: United Nations, 22 January 2001.

United Nations. General Assembly. *Resolution 53/70 - Developments in the field of information and telecommunications in the context of international security.* A/RES/53/70. New York: United Nations, 4 January 1999.

United Nations. General Assembly. *Resolution S-20/4 - Measures to enhance international cooperation to counter the world drug problem.* A/RES/S-20/4*. New York: United Nations, 21 October 1998.

United Nations. Institute for Disarmament Research. Agenda – Information & Communication Technologies and International Security – 24-25 April 2008. Last accessed 12 October 2011.
<http://www.unidir.org/pdf/activites/pdf-act371.pdf>

United Nations. Institute for Disarmament Research. "Conference – Developments in the field of information and telecommunication in the context of international security". Last accessed 12 October 2011.
< http://www.unidir.org/bdd/fiche-activite.php?ref_activite=81>

United Nations. Institute for Disarmament Research. "Conference – Information and Communication Technologies and International Security". Last accessed 12 October 2011.
<http://www.unidir.org/bdd/fiche-activite.php?ref_activite=371>

United Nations. Institute for Disarmament Research. "ICTs and International Security" Disarmament Forum 3 (2007). Last accessed 12 October 2011. <http://www.unidir.org/bdd/fiche-periodique.php?ref_periodique=1020-7287-2007-3-en#contents>

United Nations. Institute for Disarmament Research. "Research Project – Group of

Governmental Experts on the Issue of Information Security (2009-2010)". Last accessed 12 October 2011.
<http://www.unidir.org/bdd/fiche-activite.php?ref_activite=483>

United Nations. Institute for Disarmament Research. "Research Project – Perspectives on Cyber War: Legal Frameworks and Transparency and Confidence Building". Last accessed 12 October 2011.
<http://www.unidir.org/bdd/fiche-activite.php?ref_activite=583>

United Nations. Institute for Disarmament Research. *Summary - Developments in the field of information and telecommunication in the context of international security*. Last accessed 12 October 2011.
<http://www.unidir.org/pdf/activites/pdf2-act81.pdf>

United Nations. International Telecommunication Union."Child Online Protection". Last accessed 12 October 2011.
<http://www.itu.int/osg/csd/cyber-security/gca/cop/meetings/june-tokyo/bios/index.html>

United Nations. International Telecommunication Union.*Cybersecurity for all – Global Cybersecurity Agenda: A Framework for International Cooperation.* Geneva: United Nations, March 2010.

United Nations. International Telecommunication Union.*ITU Global Cybersecurity Agenda: High Level Experts Group – Global Strategic Report.* Geneva: United Nations, 2008.

United Nations. International Telecommunication Union. "Overview of cybersecurity – Recommendation ITU-T X.1205". *Series X: Data Networks, Open System Communications and Security" – Telecommunication security*. Geneva: United Nations, April 2008.

United Nations. International Telecommunication Union. "PowerPoint Presentation on Global Cybersecurity Agenda to Open-ended Intergovernmental Expert Group on Cybercrime – Vienna, 17- 21 January 2011". Last accessed 8 October 2011.

<https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/I TU_Cyber crime_ EGMJan2011.pdf>

United Nations. Internet Governance Forum."About the Internet Governance Forum". Last accessed 12 October 2011. <http://www.intgovforum.org/cms/aboutigf>

United Nations. Internet Governance Forum."Past Staff Members". Last accessed 12 October 2011. <http://www.intgovforum.org/cms/component/content/article/762-past-staff-members>

United Nations. Interregional Crime and Justice Research Institute. "Cybercrimes - UNICRI's Initiatives". Last accessed 12 October 2011. <http://www.unicri.it/emerging_crimes/cybercrime/initiatives/>

United Nations. Office on Drugs and Crime. "Law enforcement officers trained to tackle cybercrime". (19 June 2009) Last accessed 12 October 2011. <https://www.unodc.org/unodc/en/frontpage/2009/June/law-enforcement-officers-trained-in-tackling- cybercrime.html>

United Nations. Office on Drugs and Crime."Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime - Vienna, 17-21 January 2011". Last accessed 12 October 2011. <https://www.unodc.org/unodc/en/expert-group-to-conduct-study-cybercrime-jan- 2011.html>

United Nations. Office on Drugs and Crime."Secretariat to the Governing Bodies Section". Last accessed 12 October 2011. <https://www.unodc.org/unodc/en/commissions/secretariat2.html?ref=menuside>

United Nations. Security Council. Counter-Terrorism Committee. "About Us". Last accessed 12 October 2011. <http://www.un.org/en/sc/ctc/aboutus.html>

United Nations. Unicef. "Child protection from violence, exploitation and abuse". Last accessed 12 October 2011.

<http://www.unicef.org/protection/57929_57985.html>

United Nations. World Summit on the Information Society.*Report of the Tunis phase of the World Summit on the Information Society, Tunis, KramPalexpo, 16-18 November 2005.*WSIS- 05/TUNIS/DOC/9Rev.1)-E. Tunis: United Nations, 15 February 2006.

Wegener, Henning. "Cyber Peace", in *The Quest for Cyber Peace*. International Telecommunication Union and World Federation of Scientists, January 2011.

Wegener, Henning. "Harnessing the perils in cyberspace: who is in charge?" *Disarmament Forum* 3 (2007) Last accessed 12 October 2011. <http://www.unidir.org/pdf/articles/pdf-art2645.pdf>

Wikipedia. "History of the Internet". Last accessed 12 October 2011. <https://secure.wikimedia.org/wikipedia/en/wiki/History_of_the_Interne>

World Federation of Scientists."The Erice Statement". Last accessed 12 October 2011. <http://www.federationofscientists.org/WfsErice.asp>

World Federation of Scientists. *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar.*
WSIS-03/GENEVA/CONTR/6. World Summit on the Information Society, 2003.

Wu, Tim and Jack Goldsmith. *Who Controls the Internet – Illusions of a Borderless World.* Oxford: Oxford University Press, 2008.

访谈

Bosco, Francesca. Project Officer. United Nations Interregional Crime & Justice Research Institute. Email correspondence with author. September 2011.

Chiesa, Raoul. Senior Advisor, Strategic Alliances & Cybercrime Issues. United Nations Interregional Crime & Justice Research Institute. Email correspondence with author and interview with author. Turin, Italy. August 6, 2010.

Neutze, Jan. Programme Officer. Counter-Terrorism Implementation Task Force.

United Nations. Phone interview with author. August 30, 2010.

Ntoko, Alexander. Head of Corporate Strategy Division.International Telecommunications Union. Email correspondence with author and interview with author. Geneva, Switzerland. August 3, 2010.

一些受访官员希望匿名。

附录 1

大会决议

57/239. 创造全球网络安全文化

大会，[…]注意到本决议附件所列的要点，以期创造全球网络安全文化[…]

2002 年 12 月 20 日

第 78 次全体会议

附件
创造全球网络安全文化的要点

信息技术的迅速进步改变了研制、拥有、提供、管理、维修和使用信息系统和网络的各国政府、商业、其他组织和个别使用者(“参与者”)对待网络安全的方式。如要创造全球网络安全文化，所有参与者均须注意下列九项相辅相成的要点：

(a) 意识。参与者应意识到信息系统和网络安全的必要性以及他们在增进安全方面所能做的工作；

(b) 责任。参与者应以适合其个别角色的方式对信息系统和网络的安全负责。他们应定期审查各自的政策、惯例、措施和程序，并评估这些政策、惯例、措施和程序是否与其环境相称；

(c) 反应。参与者应及时地协力预防和侦查安全事件并对这些事件作出反应。他们应酌情分享关于威胁和脆弱性的信息，实施开展迅速、有效合作的程序，预防和侦查安全事件并对这些事件作出反应。这方面可能涉及跨边界的信息分享和合作；

(d) 道德。鉴于信息系统和网络在现代社会的普遍性，参与者需要尊重别人的正当利益并认识到他们的行动或不行动可能危害别人；

(e) 民主。应以符合民主社会所确认的价值观的方式实施安全，这些价值观包括交流思想和意见的自由、信息的自由流动、信息和通信的机密性、个人资料的适当保护、公开性和透明度；

(f) 风险评估。所有参与者应定期进行风险评估，这些评估应：指出各种威胁和弱点；基础广泛，足以包含关键的内外因素，例如技术、物质和人的因素、政策及涉及安全问题的第三方服务；能够确定可接受的风险水平；协助选择适当的控制手段，根据所要保护的信息的性质和重要性，管理可能对信息系统和网络造成危害的风险；

(g) 安全设计和实施。参与者应将安全视为信息系统和网络的规划和设计、操作及使用的一项基本要素；

(h) 安全管理。参与者应以全面方式对待安全管理，这种方式基于动态的风险评估，其中包括参与者在各级进行的活动及其业务的所有方面；

(i) 再行评估。参与者应审查和再行评估信息系统和网络的安全，并对安全政策、惯例、措施和程序作出适当的修改，以便应付新的、不断演变的威胁和弱点。

附录 2

大会决议

58/199. 创造全球网络安全文化及保护重要的信息基础设施

大会，[…]注意到本决议附件所列保护重要信息基础设施的要点[…]

2003 年 12 月 23 日

第 78 次全体会议

附件
保护重要信息基础设施的要点

1. 建立有关网络脆弱性、威胁和事故的紧急警报网。

2. 加强宣传，以便利益有关者了解其重要信息基础设施的性质和范围及其在保护工作中必须发挥的作用。

3. 检查基础设施，确定其中的相互依存关系，以便加强对此类设施的保护。

4. 推动公共和私营部门的利益有关者建立伙伴关系，交流和分析重要基础设施信息，以便预防、调查和应对此类基础设施受到的损害或攻击。

5. 建立、维持和测试应急通信网，确保它们在紧急情况中保持安全和稳定状态。

6. 确保关于提供数据的政策考虑到保护重要信息基础设施的必要性。

7. 为追查攻击重要信息基础设施的行为提供方便，并酌情向其他国家披露追查情报。

8. 开展培训和演习活动以增强应对能力，测试信息基础设施受到攻击时的连续性能和应急计划，并鼓励利益有关者参与类似活动。

9. 具有充分的实体法和程序法以及训练有素的人员，以使国家能够调查和起诉攻击重要信息基础设施的行为，并酌情与其他国家协调此类调查。

10. 酌情参与国际合作以保障重要信息基础设施的安全，合作方式包括拟订和协调紧急警报系统，交流和分析有关脆弱性、威胁和事故的情报，并根据国内法律协作调查攻击此类基础设施的行为。

11. 促进国家和国际两级的研究和开发，鼓励采用那些符合国际标准的安全技术。

附录 3

大会决议

64/211. 创建全球网络安全文化以及评估各国保护重要信息基础设施的努力

大会，[…] 邀请各会员国在其认为适当时利用所附国家保护重要信息基础设施努力自愿自我评估工具，协助评估本国在这方面以及为加强其网络安全作出的努 力，以突出说明有待采取进一步行动的领域，目标是提升全球网络安全文化[…]

2009 年 12 月 21 日

第 66 次全体会议

附件
国家保护重要信息基础设施努力自愿自我评估工具[175]

评估网络安全需要和战略

1. 评估信息和通信技术在贵国国民经济、国家安全、重要基础设施(如运输、水和食物供应、大众保健、能源、金融、应急服务)以及民间社会中的作用。

2. 确定贵国经济、国家安全、重要基础设施和民间社会在网络安全和重要信息 基础设施保护方面面临并且必须加以管理的风险。

3. 了解已投入使用网络的弱点、每个部门目前所面临威胁的相对严重程度和现行管理计划；说明经济环境、国家安全优先事项以及民间社会需求等因素的变化 如何影响这些评估。

4. 确定国家网络安全和保护重要信息基础设施战略的目标，叙述该战略的目标、目前的实施程度、衡量进展情况的指标、该战略与其他国家政策目标的关系 以及该战略在各区域和国际举措中的作用。

175这是会员国认为适当时可以部分或全部采用的自愿工具，以协助它们努力保护国家重要的信息基础设施和加强国家网路安全。

利益攸关方的作用和责任

5. 确定在网络安全和保护重要信息基础设施方面发挥作用的关键利益攸关方，并叙述每个利益攸关方在制定有关政策和开展有关行动方面的作用，包括：

- 国家政府各部委或机构，并说明主要联系人和各自的责任；
- 其他(地方和地区)政府参与方；
- 非政府行动者，包括工商界、民间社会和学术界；
- 公民，并指出因特网普通用户是否可获得避免网上威胁的基本培训，是否已开展关于网络安全的全国提高认识运动。

政策制定过程和参与

6.说明在政府-行业协作制定网络安全和保护重要信息基础设施政策和开展这项活动方面现有的正式和非正式协作渠道；列明参与方、各方的作用和目标、获取和处理投入的方法以及这些投入是否足以实现相关的网络安全和保护重要信息基础设施目标。

7. 说明可能需要进一步建立的其他论坛或结构，以整合必要的政府和非政府观点和知识，实现国家网络安全和保护重要信息基础设施目标。

公私合作

8. 汇集发展政府与私营部门合作方面所有已采取的行动和已制定的计划，包括 任何信息分享和事件管理安排。

9. 汇集促进共同依赖相同互联重要基础设施的重要基础设施参与方和私营部 门行动者的共同利益和处理其共同挑战的所有现行举措和计划举措。

事件管理和恢复

10. 说明担任事件管理协调者的政府机构，包括监视、预警、应对和恢复等职能的能力；参与合作的政府机构；参与合作的非政府参与方，包括行业和其他合作伙伴；已作出的合作和可靠信息共享安排。

11. 另行说明国家一级计算机事件应对能力，包括确认国家级电子计算机事件应对小组及其作用和责任，包括保护政府计算机网络的现有工具和程序以及传播事 件管理信息的现有工具和程序。

12. 说明可增强事件应对和应急规划能力的国际合作网络和进程，同时酌情说明各合作伙伴和各种安排，以促进双边和多边合作。

法律框架

13. 审查和更新由于新信息和通信技术迅速发展并且由于依赖这些新技术而可 能过时或失效的法律依据(包括有关网络犯罪、隐私、数据保护、商业法、数字签名和加密的法律依据),在审查过程中利用区域和国际公约、安排和先例。确定贵国是否制定了调查和起诉网络犯罪的必要立法,注意到现有框架,例如联合国大会关于打击非法滥用信息技术的第 55/63 号和第 56/121 号决议和包括欧洲委员会《网络犯罪问题公约》在内的区域倡议。

14. 确定贵国有关网络犯罪的依据和程序,包括法律依据和国家防止网络犯罪部门的现状,以及检察官、法官和议员对网络犯罪问题的认识程度。

15. 评估现行法规和法律依据是否足以处理网络犯罪以及更广泛的网络空间当前和未来的挑战。

16. 检查贵国参与国际社会打击网络犯罪的努力,例如参加打击赛博犯罪全天候联络点网络的情形。

17. 确定在基础设施设在本国境内或罪犯居住在本国境内而受害者居住在其他地方的情形下,国家执法机构要求满足哪些条件,才与国际同行合作调查跨国网络犯罪。

发展全球网络安全文化

18. 总结为发展大会第57/239和58/199号决议所述国家网络安全文化而采取的行动和制定的计划,包括政府运作系统网络安全计划、对儿童和个人用户等方面开展的全国提高认识方案和外联方案的执行情况以及国家网络安全和保重要信息基础设施的培训要求。

附录 4

2011 年 9 月 12 日中国、俄罗斯联邦、塔吉克斯坦和乌兹别克斯坦常驻联合国代表给秘书长的信的附件(A/66/359)

附件 C
信息安全国际行为准则

大会，

回顾其关于科学和技术在国际安全领域的作用的各项决议，除其他外，确认科学和技术的发展可以有民用和军事两种用途，需要维持和鼓励民用科学和技术的进展；

注意到在发展和应用最新的信息技术和电信手段方面取得了显著进展；认识到应避免将信息通信技术用于与维护国际稳定和安全的宗旨相悖的目的，从而给各国国内基础设施的完整性带来不利影响，危害各国的安全；

强调有必要加强各国的协调和合作打击非法滥用信息技术，并在这方面强调联合国和其他国际及区域组织可以发挥的作用；

强调互联网安全性、连续性和稳定性的重要意义，以及保持互联网及其他信息通信技术网络免受威胁与攻击的必要性。重申必须在国家和国际层面就互联网安全问题达成共识并加强合作；

重申与互联网有关的公共政策问题的决策权是各国的主权。对于与互联网有关的国际公共政策问题，各国拥有权利并负有责任；

认识到可以放心安全地使用信息和通信技术是信息社会的一大支柱，必须鼓励、推动、发展和大力落实全球网络安全文化，正如第 64 届联合国大会第 64/211 号决议：“创建全球网络文化以及评估各国保护关键信息基础设施的努力”序言第 4 段所指出的；

指出必须加强努力，通过便利在网络安全最佳做法和培训方面向发展中国家转让信息技术和能力建设，弥合数字鸿沟，正如第 64 届联合国大会第 64/211 号决议：“创建全球网络文化以及评估各国保护关键信息基础设施的努力”序言第 11 段所指出的。

通过以下信息安全国际行为准则：

目标与适用范围

本准则旨在明确各国在信息空间的权利和责任，推动各国在信息空间采取建

设性和负责任的行为，促进各国合作应对信息空间的共同威胁与挑战，确保信息通信技术包括网络仅用于促进社会和经济全面发展及人民福祉的目的，并与维护国际和平与安全的目标相一致。

本准则对所有国家开放，各国自愿遵守。

行为准则

所有自愿遵守该准则的国家承诺：

(a) 遵守《联合国宪章》和公认的国际关系基本准则，包括尊重各国主权，领土完整和政治独立，尊重人权和基本自由，尊重各国历史、文化、社会制度的多样性等。

(b) 不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。

(c) 合作打击利用信息通信技术包括网络从事犯罪和恐怖活动，或传播宣扬恐怖主义、分裂主义、极端主义的信息，或其他破坏他国政治、经济和社会稳定以及精神文化环境信息的行为。

(d) 努力确保信息技术产品和服务供应链的安全，防止他国利用自身资源、关键设施、核心技术及其他优势，削弱接受上述行为准则国家对信息技术的自主控制权，或威胁他国政治、经济和社会安全。

(e) 重申各国有责任和权利依法保护本国信息空间及关键信息基础设施免受威胁、干扰和攻击破坏。

(f) 充分尊重信息空间的权利和自由，包括在遵守各国法律法规的前提下寻找、获得、传播信息的权利和自由。

(g) 推动建立多边、透明和民主的互联网国际管理机制，确保资源的公平分配，方便所有人的接入，并确保互联网的稳定安全运行。

(h) 引导社会各方面理解他们在信息安全方面的作用和责任，包括本国信息通信私营部门，促进创建信息安全文化及保护关键信息基础设施的努力。

(i) 帮助发展中国家提升信息安全能力建设水平，弥合数字鸿沟。

(j) 加强双边、区域和国际合作。推动联合国在促进制定信息安全国际规则、和平解决相关争端、促进各国合作等方面发挥重要作用。加强相关国际组织之间的协调。

(k) 在涉及上述准则的活动时产生的任何争端，都以和平方式解决，不得使用武力或以武力相威胁。