联合国 A/64/129

大会

Distr.: General
8 July 2009
Chinese
Original: English/Russian/Spanish

第六十四届会议

暂定项目表* 项目 90

从国际安全的角度来看信息和电信领域的发展

从国际安全的角度来看信息和电信领域的发展

秘书长的报告

目录

* A/64/50。

09-39632 (C) 300709 310709

一. 导言

1. 大会在第 63/37 号决议第 3 段中请所有会员国继续向秘书长通报它们对下列问题的看法和评估意见：

(a) 对信息安全问题的一般看法；

(b) 在国家一级为加强信息安全和促进这一领域的国际合作所作的努力；

(c) 该决议第 2 段中提及的有关概念的内容；

(d) 国际社会为加强全球一级的信息安全可能采取的措施。

2. 按照这项要求，于 2009 年 2 月 27 日向会员国寄发了一份普通照会，请它们就这一主题提供资料。所收到的答复载于下文第二节。以后再收到的其他答复将作为本报告增编印发。

二. 从各国政府收到的答复

巴西

[原件：英文]
[2009 年 6 月 11 日]

1. 信息和电信是现代社会不可或缺的一个组成部分，因为现代社会在很大程度上有赖于信息和电信。当今社会的活动时时刻刻都严重依赖此类服务，从而使它们成为极其宝贵的资源，对国家的富强和繁荣至关重要。

2. 技术进步使得这种情形成为了现实，但同时也造成了国际安全方面的诸多问题。鉴于当今社会对于信息获取和电信基础设施的依赖性与日俱增，由此产生的新的安全漏洞可能在军事冲突、犯罪和恐怖活动中受到利用。

3. 这种利用可能会破坏私营公司、银行、股票市场和政府组织的活动。尽管基本通信网络之间日益交织的相互联系毫无疑问是有益的，但它也带来了一系列的新问题，必须由各国在国家和国际层面予以应对。

4. 信息和电信领域的发展可能会导致安全漏洞，但同时在网络战中可以被用作资产。已经有一些国家武装部队设置了接受专门培训和配备特殊装备的军事单位，其目标是通过侵入和破坏信息网络让重要的基础设施丧失能力，甚至摧毁这些设施。根据不同的目标和采用的手段，此类攻击的效果从“软杀伤”敌人的武器或传感系统，到严重破坏全国电网不等。

5. 仅需较少的投资就能开发许多此类能力，从而提高网络的效能。鉴于这些因素，在不远的将来，网络战很可能会成为国家间军事冲突的跳板。恐怖分子或恐怖组织也可能会采用同样的策略。

6. 巴西意识到，这一议题对于维护国际和平与安全十分重要，并建议以两种不同的方式来处理这个问题。首先，国际社会应努力创立适当的工具来处理涉及信息技术的犯罪和恐怖活动。另一种方式与此不同但又相辅相成，那就是国际社会应考察网络战兴起的影响、对裁军和不扩散制度及国际战争法的可能需求，以充分考虑到这个问题的多方面影响。

7. 应当在适当的论坛上充分讨论犯罪和恐怖活动，联合国应当发挥重要作用，应会员国的要求协助它们实现以下目标：

- 建立应急和替代网络来保护关键基础设施；
- 考察网络结构，分析相互依赖关系，并确定有效的保护方法；
- 政府和私营部门之间开展密切合作，以便使各组织之间的信息流达到理想的安全水平；
- 建立保护制度，以避免或尽量减少网络攻击的影响；
- 采取各种手段和措施，以使当局能够追查网络攻击的来源；
- 就缔结具有法律约束力的网络犯罪国际文书是否可取展开辩论；
- 授予国家机构测试和评价信息系统安全级别的资格；
- 设立相关程序，在各国主管部门之间相互通报网络威胁；
- 避免歧视性机制，因为此类机制可能会妨碍各国获取电信和信息系统领域的高科技；
- 就网络安全的重要性开展教育和提高认识活动。

8. 在讨论将信息和电信用于国家间冲突局势中的网络战等问题时，联合国也应发挥主导作用，并特别注意以下几个方面：

- 信息战的鉴别、描述和分类；
- 对各种信息战武器和可以用作信息战武器的手段予以鉴别和分类；
- 订立利用信息战武器的行为准则；
- 保证所有国家都享有防止本国遭受网络攻击的平等权利；
- 编订一个联合国的词汇表，内载国际安全领域的主要信息和电信术语的定义。

哈萨克斯坦

[原件：俄文]
[2009 年 7 月 2 日]

1. 信息和通信技术在全世界人类生活的所有领域都带来了范围广泛的变化。正如《冲绳全球信息社会宪章》所述：“信息和通信技术是塑造 21 世纪的最强大的力量之一。它所带来的革命性冲击不仅影响到人们生活、学习和工作的方式，也影响到政府与民间社会开展互动的方式。”

2. 当今时代，随着科技的不断进步，已出现计算机化的明显趋势，也产生了大量的数据处理系统。因特网影响到公众和社会生活的几乎所有领域，且因特网用户持续增长。因此，信息资源、数据处理系统和计算机网络已经成为一个国家的基础设施中最易受攻击的环节。

3. 由于因特网仍然是一片实质上自由和不受控制的领地，犯罪分子正试图利用现代信息和通信技术的潜力。根据国际商会专家的估计，基于因特网的犯罪案件数量正与因特网用户的人数成正比增长。根据国际刑事警察组织(国际刑警组织)的数据，因特网社区是全球犯罪率攀升最快的领域之一。

4. 这些犯罪案件大致可以分为以下三类：

(a) 对国家安全和公共安全构成威胁的世界性、国家和公共犯罪行为(包括号召推翻现存秩序、企图贬低主权以损害独立和国家利益、恐怖主义宣传、大国沙文主义、仇外心理、一切形式的极端主义以及基于民族、种族、宗教、性别和其他原因的歧视行为)；

(b) 对个人权利和自由构成威胁的世界性民事犯罪行为(包括侵犯个人权利和自由、使用损害他人名誉的材料、向个人施加压力、败坏他人声誉、传播机密信息、使用他人的因特网服务、伪造文件和侵犯知识产权等)；

(c) 威胁到道德标准、不得体的传统犯罪行为(包括色情制品、恋童癖、其他形式的性变态行为、吸毒致瘾和酗酒等)。

5. 此类信息的出现表明，对由因特网引发的法律关系进行监管的国家立法不够充分，需要采取超国家的办法。在国际一级，仍然没有任何一个方法可以确定和评估对国际信息安全构成的威胁，也没有任何机制推动开展国际合作来应对此类威胁。与此同时，迄今为止各国在信息技术领域提出的所有国际安全概念都缺乏普世性。

6. 之所以产生这一局面，是由于最发达国家和最不发达国家之间的技术差距、潜在的政治分歧、评估网络空间最新进展和事件的互相矛盾的方式以及其他诸多因素。

7. 联合国各组织和欧洲各个组织(例如欧洲安全与合作组织)现有国际文书的主要优先领域，是由常见犯罪和恐怖主义构成的信息技术威胁。但是，这些文书都忽略了这样一种可能性：即信息技术的进步在武装冲突期间可能会遭到滥用，成为主导信息空间、威胁国家主权和民族特征的信息战工具。此类文书还忽略了对国家信息基础设施的自然和人为威胁。

8. 防止此类威胁的一个关键因素，不仅可以是与军事和政治伙伴达成国际信息安全安排，也可以是订立政治和法律协定，相互承诺不将信息用作武器、设立共同机制尽量减少损害性行为的负面影响和振兴国家信息基础设施以及其他措施。

9. 值得一提的是，哈萨克斯坦共和国的代表参与了集体安全条约组织和上海合作组织框架内正在开展的类似努力，专家们正在考察缔结相关政府间协议的可能性。特别是，根据 2007 年 8 月 16 日上海合作组织成员国元首理事会在比什凯克作出的一项决定中通过的上海合作组织确保国际信息安全的行动计划，来自上海合作组织成员国的国际信息安全专家们起草了关于开展合作确保国际信息安全的政府间协议草案。2009 年 6 月 15 日，上海合作组织成员国元首理事会在叶卡捷琳堡正式签署了这份协议。

10. 需要指出的是，在世界任何地区都没有类似的协议，而且考虑到其他国家可能会加入这份协议，协议的签署具有重大的国际意义。

11. 此外，在集体安全条约组织的框架内没有一个信息政策和信息安全问题临时工作组，该工作组向集体安全条约缔约国安全理事会秘书委员会汇报工作。该工作组拟定了联合活动方案，以便为集体安全条约组织成员国建立信息安全制度。

12. 集体安全条约组织成员国开展了联合预防演习，作为“Proksi”行动的一个组成部分，该行动基于各国安全与内务(警察)部门之间的统一合作活动方案。

13. 鉴于因特网的规模和跨境性质，我们建议联合国会员国拟订和通过一项有关信息安全的国际公约。这样一项公约的主要支柱之一，应当是为打击基于因特网的犯罪行为而开展的努力。

14. 这一文书应努力促进在信息安全领域开展互利互惠的国际合作，防止全球信息和通信系统遭受负面的地缘政治影响。

15. 公约还需要建立接收和使用信息的组织、技术、政策和社会机制，以期保护所有联合国会员国的宪政制度、国家主权和领土完整，并确保政治、经济和社会稳定、法律和秩序以及法治。公约还应纳入相关机制，保证能够行使宪法权利、人权和公民权利。

16. 在国家一级，哈萨克斯坦共和国已经草拟了一项法律草案，对涉及信息和通信网络的部分立法法令予以修订和补充。目前参议院正在审议这一法律草案。

17. 该草案拟议强化对通过信息和通信网络在哈萨克斯坦共和国境内传播信息实施管理的各种标准。

18. 在国家一级，在这一领域增进信息安全和促进国际合作的当前努力，主要是由国家安全部门开展的。发现和防止跨国计算机犯罪的活动正在不断开展。

19. 例如，俄罗斯联邦国家安全委员会和联邦安全局在 2008 年制止了一个跨国有组织犯罪团伙的黑客活动，该团伙通过威胁对经营网上业务的公司发起“分布式拒绝服务攻击”，从这些公司勒索了大量资金。

20. 在信息安全领域开展的预防演习说明，一些基于因特网的新形式犯罪已初现端倪，如敲诈勒索、贩运人口、拉皮条、传播宣扬色情、残暴、暴力行为、恐怖主义和极端主义的材料等。

21. 例如，2008 年共发现了 45 起传播色情材料的案例。另外，还应注意在因特网上的儿童色情材料越来越多的情况：在 2005-2006 年期间共发现了一起传播儿童色情材料的案例；2007 年发现了 7 起；2008 年则发现了 14 起，其中 2 起来自哈萨克斯坦的因特网社区。

22. 值得一提的是，由于缺乏明确的信息安全议题立法框架，打击信息安全和高技术犯罪的努力并不充分。

23. 必须考虑到当前的现实情况，进一步改进这一领域的现有监管和法律条例。

24. 在我们看来，根据发达国家的经验，为加大对此类犯罪行为的惩罚力度，有必要对现有的刑法予以更新。

25. 此外，考虑到计算机犯罪的跨境性质，执法部门必须不断扩大其行动协调领域，以确保对因特网攻击行为作出快速反应。哈萨克斯坦执法部门与其他国家特别事务部门和执法部门合作发现，来自哈萨克斯坦因特网社区的计算机攻击活动有所增长。与此同时，因特网攻击行为的受害者在汇报攻击信息时很难作出快速反应，因为和其他设有因特网信息安全中心(通常称为计算机应急小组)的国家不同，哈萨克斯坦共和国有关机构并没有设置负责接受和转递计算机事件情况的官方部门。

26. 在这方面，我们认为执法机构应设立特定专门部门，负责查明、打击和侦测与信息安全有关的犯罪行为。这些部门应配备打击此类犯罪行为的先进工具。

27. 哈萨克斯坦已经为根据题为“从国际安全的角度来看信息和电信领域的发展”的大会第 63/37 号决议第 4 段设立的政府专家组提名人选。

黎巴嫩

[原件：英文]
[2009 年 5 月 22 日]

1. 我们正在公布一项新的、关于黎巴嫩信息和通讯技术部门的法律，该法目前处在国民议会最后核准阶段。该法将涵盖所有相关事项，包括安全和有关信息犯罪的所有事项。

2. 一旦上述法律生效，电信部将与其他部委和所有有关负责人一道安排与[第 63/37 号决议第 3 段](b)、(c)和(d)分段有关的事项。

立陶宛

[原件：英文]
[2009 年 5 月 26 日]

1. 立陶宛在其国家和国际议程中均高度重视信息安全问题。网络安全问题是国家安全的一个重要组成部分。

2. 为加强保护通信和信息系统并提高认识，在国际一级开展合作是十分重要的。在联合国、欧洲联盟、北大西洋公约组织和欧洲安全与合作组织等国际组织的议程中，信息安全问题正获得越来越多的关注，立陶宛欣见这一发展，并积极参与这些组织处理这一问题的工作。立陶宛各有关机构与其合作伙伴开展了密切的合作。自 2004 年 7 月 1 日起，立陶宛成为欧洲委员会《网络犯罪公约》的缔约国。

3. 立陶宛是发起设立爱沙尼亚塔林“北约合作网络防御英才中心”的 7 个北约成员国之一，该中心于 2008 年 5 月 14 日获得了北约英才中心地位。

4. 2005 年 3 月 11 日，欧洲议会和欧洲委员会通过决定，采纳了称为“互联网加强安全”的多年度共同体方案，借以促进互联网使用安全和开发新的在线技术。该方案的主要任务是在加强互联网安全和实施热线电话等问题上教育社会公众。

5. 在 2008 年 5 月 28 日和 29 日在都柏林举行的国际互联网热线协会大会上，立陶宛成为了国际互联网热线协会的成员。

6. 在国家一级，立陶宛在 2000 年对信息基础设施的状况进行了第一次评估，这标志着立陶宛着手处理这一问题的复杂过程从此启动。主要的评估领域包括各国家机构对信息安全问题的理解水平、现有的政策和网络保护的水平。

7. 立陶宛共和国政府的决议指定立陶宛共和国内政部为国家各个机构的信息技术安全协调中心(2001 年 3 月 14 日，第 291 号决议)。

8. 立陶宛根据《国家信息技术安全战略》(至 2004 年)和《国家机构电子信息安全国家战略》(至 2008 年)的规定，制定和实施了一系列措施，以保障信息安全。

9. 2008 年 6 月 17 日，立陶宛总理颁布了一项法令，成立了网络安全问题机构间工作组。2008 年 11 月 21 日，工作组向政府提交了一份报告，报告中载有改善立陶宛网络安全的提案和建议。

10. 立陶宛政府计划在不久的将来拟订《电子通讯网络和信息安全法》草案和新的《电子信息安全战略》，以期进一步提高信息安全(特别是网络防御)方面的国家能力。上述战略的目标包括：提高体制结构作为抵御网络攻击的框架的效率，增强数据传输基础设施的安全性和复原力，有效防止重要信息基础设施遭受网络威胁，借助第二方和第三方审计政策确保各方严格遵守各项政策和要求。

11. 2005 年以来，立陶宛通信管理局开展了多次电子通信网络和信息安全调查，以解决悬而未决的问题。通信管理局承担国家计算机应急小组的职能。

12. 立陶宛国家计算机应急小组的任务是通过预防、观察和解决信息安全事件并传播有关信息安全威胁的信息，促进信息社会的安全。2008 年 9 月 30 日，新的网站 www.cert.lt 正式开放。2009 年 1 月 16 日，立陶宛国家计算机应急小组成员成为“可信介绍人”(欧洲的计算机安全事故应变小组和计算机应急小组的信任网络)的认证成员。

13. 立陶宛努力确保国际社会继续高度重视信息安全问题并加大解决这一问题的力度。立陶宛致力于积极参与国际社会今后为实现更大信息安全而作出的努力，并努力为此作出贡献。

墨西哥

[原件：西班牙文]
[2009 年 6 月 8 日]

1. 有关安全问题的主要认识涉及到：各国国防体系的信息系统可能存在薄弱点；恐怖主义分子将信息技术和电信设施用于暴力或阻吓目的的风险客观存在。

2. 在此背景下，墨西哥出于对世界电信安全发展情况的忧虑，出席了 2008 年 10 月在南非举行的世界电信标准化大会，并与美洲电信委员会的其他成员国(加拿大、巴拉圭和乌拉圭)一道，提交了一份决议草案，邀请各所大学积极参与国际电信联盟的会议，以加强其工作。

3. 此外，在区域范围内，墨西哥担任了美洲电信委员会常设执行委员会第二十届会议的副主席。在这次会议期间，墨西哥通过联邦电信委员会向区域各国提供

了一套有关有害干预卫星系统问题的课程。各国一致同意于 2010 年第一季度在墨西哥举行美洲电信委员会第五届常会。

4. 墨西哥采取了多项措施加强信息和通信领域的国际安全，包括成立了一个网络警察部门。该部门除针对借助因特网和其他信息技术工具犯下的罪行采取预防措施之外，还具体注重防止侵害未成年人的犯罪行为，并处理关于此种行为的报告。

塞尔维亚

[原件：英文]
[2009 年 6 月 9 日]

1. 各国有必要在网络空间领域巩固本国的法律规范，因为网络空间已不再局限于一国境内，参与扰乱和(或)滥用信息和电信系统的个人和(或)团体往往可能并不在事发国。这份决议迈出了第一步，打下一个坚实的基础，据此可兼顾各方的各种建议，在国际上统一立法加强国际安全，同时又保证信息自由流动。

2. 有必要制定更严厉的法律，在国家一级尤其如此，这些法律必须与用户的技术技能和教育水平相应，并辅以对用户的持续教育，并建立专门机构来计划、组织和控制这一领域的技术因素。

3. 在评估信息和电信系统领域的信息安全原则方面，要点如下：

问题

- 每天都会产生新类型的恶意程序，威胁到信息和电信系统的安全
- 有黑客多次试图攻击塞尔维亚共和国国防和武装力量部的官方网站
- 在互联网上宣传恐怖主义观点

安全程序与合作

- 在塞尔维亚共和国国防和武装力量部使用信息和电信系统的所有层次应用适当的反病毒软件
- 继续防止黑客袭击塞尔维亚共和国国防和武装力量部的官方网站
- 参与旨在提高对网络犯罪和网络恐怖主义威胁的认识的会议和研讨会

建议

建立一个国际机构，担负以下责任：

- 评估数据和电信通道保护的问题
- 监测国际网络恐怖主义和网络犯罪领域的“威胁”因素

- 评估信息电信系统领域的国际安全问题，并就解决方案提出建议
- 制定教育方案，以期提高对网络犯罪和网络恐怖主义危险的认识
- 在政府间举行知识和经验交流

塔吉克斯坦

[原件：英文]
[2009 年 5 月 20 日]

1. 如今，电信领域被视为任何国家发展经济和实现稳定与安全的一个重要因素。

2. 塔吉克斯坦为电信领域的发展提供了所有必要的条件，允许自由竞争。为各不同运营商与服务提供商发放牌照，并引进新的服务。

3. 至关重要的是，必须确保信息和电信基础设施的运行安全，增强对企业信息系统的保护，并借此对抗散布恐怖主义、极端主义和暴力等意识形态的传播。

4. 塔吉克斯坦已经做好支持上述举措的准备，并将在推进国际信息安全领域通力合作。

泰国

[原件：英文]
[2009 年 6 月 3 日]

对信息安全问题的一般看法

1. 当今世界已经进入信息社会时代，人们利用信息技术使生活变得更加方便，例如在金融交易、新闻和信息交流等领域。然而，信息技术不仅带来了裨益，同样也给某些团体以非法和不道德的手段利用信息技术提供了契机，从而引发了各种各样的问题，如通过信息系统窃取情报、网络攻击、伪造电子文件、渗透政府数据库、窃取个人资料及侵犯隐私等。但是，每个国家的经济发展都离不开信息和通信技术。技术复杂程度的提高、缺乏训练有素的信息安全人员和充足的资源，都可能会导致计算机系统和网络的信息安全程度降低，从而致使人们失去信任，在银行、电子商务和管理等领域特别如此。因此，有必要找出和预测其中涉及的问题，以采取保障措施和安全措施，防止这些风险。为了实现这一目标，各国应相互合作，在信息安全领域采取措施，制订一个供所有国家遵守的国际标准。

在国家一级为加强信息安全和促进这一领域的国际合作所作的努力

2. 泰王国政府已将国家安全政策设为佛历年 2552 年至 2554 年(公历 2009-2011 年)泰王国政府战略规划的优先政策领域之一。目前，政府已通过法律措施来促

进信息安全，以防止信息网络被用于不道德的目的，防止其影响国家安全。这些措施包括涉及计算机犯罪、电子交易、电子签名和电子资金转帐的法律。

3. 信息和通信技术部对于确保互联网网络的信息安全、对于解决不当和非法网站的问题高度重视，并已成立一个互联网安全运营中心，其目的是监测信息技术的威胁，并与其他机构协调处理利用信息网络对国家安全构成威胁的问题。该中心的另一个目标在于制止非法利用信息网络和设立一个针对病毒与垃圾邮件的监测系统。

4. 在国际合作方面，应设立一个协调机构作为协调中心。该机构应制定相关政策，以防止和打击不当信息，采取措施应对信息安全威胁，并采取预防措施作为联合行动的指导方针。

考察旨在加强全球信息和电信系统安全的有关国际概念

5. 有必要制订促进全球信息安全的共同国际概念和原则，因为当今的网络世界互通互联、弗远无界。因此，出现在一个国家的信息安全问题可能会蔓延和影响到另一个国家。

国际社会为加强全球的信息安全可能采取的措施

6. 国际社会可以采取的措施包括开展信息交流、交流各种预防措施和应对信息安全威胁的措施。同时也应加强合作，使各国的信息技术能力发展到平等的水平，特别是发达国家应向欠发达国家转让技术和知识，以帮助后者建设能力。此外还应设立培训方案，涵盖提高认识、预防、检测、管理和应对等问题，以尽量减少信息安全风险和威胁。

7. 此外，还有必要建立一个协调机制，将各有关机构的工作联结在一起，使国家信息安全的领导和政策达到一定的标准，并朝着共同的方向前进。

8. 应当鼓励一些国际机构——例如国际电信联盟(国际电联)——促进加强信息安全领域的国际合作。国际电联举办了一次国际会议交流经验教训和探索相关措施，以解决滥用信息技术所引发的问题。此外还成立了研究小组，探索加强信息安全的措施，各国政府和有关机构可以应用和利用这些小组的研究成果。

9. 每个国家均应在业已成功设立计算机应急小组的国家的协助下，建立计算机应急小组。

10. 应当讨论每一个国家防止重要基础设施遭受网络攻击以及国际社会迅速援助或合作的问题，并共同探讨如何解决或最大程度降低此类风险的措施。

11. 应鼓励在联合国进一步增强对信息安全问题的认识，办法或许可以是通过讨论有关信息战的可能规则和条例，并发布有关信息安全威胁和漏洞的年度报告。

乌克兰

[原件：俄文]
[2009 年 5 月 20 日]

1. 信息技术在社会各个活动领域发挥着越来越大的作用，这引发了人们对于信息安全的忧虑。随着发达的信息技术进入各国和各个社会的日常生活，企图实施犯罪行为的犯罪分子和个人也更有机会针对信息与电信系统、国家机构的信息资源和商业实体发起网络攻击。

2. 在所有有记录的计算机犯罪当中，有半数涉及到非法获取计算机信息的行为。出于牟利目的的计算机犯罪不断增加，由此所造成的物质损失也在增加。跨国黑客集团犯罪也在增加。

3. 计算机犯罪很少得到报道，完整确定此类罪行的努力通常也一波三折，因为遭受此类攻击的政府和商业实体为了不冒丧失权威的风险，总是试图隐瞒这一事实，而且它们也不愿披露已遭受的损失及其信息保护系统的弱点。因此，此类犯罪案件往往未能获得报道，这说明有必要采取协调一致的预防性措施，这种措施应是信息保护系统的核心。

4. 计算机犯罪通常仅仅是一系列犯罪行为(如盗窃、勒索、欺诈等传统犯罪类型)的先声。这些犯罪行为正变得日益诡秘老练，其实施手段也在不断改进，在全球几乎所有国家都造成了巨大的经济和政治损害。此外，大多数专家认为国家的信息主权是与国家安全事务直接联系在一起的。

5. 在信息技术领域打击犯罪行为的努力遭遇了许多法律问题，导致这些问题的是计算机证据的非实物性和往往稍纵即逝的特性。在处理网络犯罪中遭遇的问题方面涉及的复杂议题，使得开展国际合作更有必要。因此，所有国家最终都必须设立适当的、相互兼容的法律、程序和规范性工具。

6. 在实践中，计算机犯罪的调查工作表明，在各国执法机构之间亟需开展合作。

7. 在国际实践中，通常会采取联合措施调查计算机犯罪。乌克兰国家安全部积极参与执法部门和特别事务部门采取的联合行动，作为打击通过因特网实施的儿童色情和诈骗行为的努力的一部分。

8. 此外，还必须加大努力，在提供信息安全、保护共同利益和引入信息安全保护举措(主要以双边和多边协议的形式)等方面进一步发展合作。特别鉴于所需法律基础业已就位，只有在各国政府机构之间开展有效合作的情况下，才能找到信息安全问题的有效解决方案。

9. 鉴于打击网络犯罪和网络恐怖主义的需要，乌克兰国家安全部与外国执法机构和特别事务部门保持联系。

10. 必须指出，网络犯罪分子往往选择政府办事处设立的网络作为袭击的目标。此外，追踪和惩罚犯罪分子的努力是否成功，取决于是否建立了高质量的国际联系，取决于国家立法是否得到了优化，能够满足现有的标准。

11. 我们与荷兰王国警务部门和俄罗斯联邦安全局合作，在 2008 年底开展了一次协调行动，制止了一个国际黑客犯罪团伙的非法活动。该团伙通过对多个金融信贷机构的自动化系统实施未经授权的干扰，从这些机构的客户那里窃取资金。

12. 考虑到全球范围内计算机犯罪不断增长、各国的黑客犯罪团伙之间存在联系以及网络威胁超越国界的事实，在打击网络威胁的过程中扩大国际合作至关重要。

13. 根据国际《网络犯罪公约》的规定，业已建立一个完全可行和方便的机制，该机制采取的形式是每周 7 天、每天 24 小时的网络，其国家联络点横跨八国集团各国和《公约》覆盖的其他国家。

14. 根据乌克兰总统关于在国家安全部内部设立 24/7 联络点(一个由国家安全部的工作人员构成的跨部门工作组)的决定，内政部、检察官办公室和司法部正在草拟一项对批准《网络犯罪公约》的法令进行修订的法案、一项对《电信法》进行修订的法案和一项有关国家安全部结构与总体人员配置的法案，以及一项关于 24/7 联络点各项职能的组织状况的总统令。

15. 作为总统决定实施过程的一个组成部分，国家安全部目前正采取步骤在国际网络内注册联络点。

16. 迄今为止完成的工作，应能使联络点有能力更加有效和以更高效率处理在世界范围内就打击网络犯罪问题开展交流与合作的问题。

17. 为了实施信息社会世界首脑会议的决定(第一阶段于 2003 年 12 月 10 日至 12 日在日内瓦举行；第二阶段于 2005 年 11 月 16 日至 18 日在突尼斯举行)乌克兰通过了一项有关在 2007-2015 年期间发展信息社会的基本原则的法律。该法律提出的基本优先事项是融入全球信息环境和发展信息社会。该法律旨在使最新的信息和通信技术能被用于营造出更加安全的氛围。

18. 此外，乌克兰还拟订和通过了一项发展电信部门的计划。该计划为后勤和技术方面的努力作出了规定，以确保乌克兰电信基础设施的所有组成部分都能安全地开展业务，其中包括：

- 通过技术手段和加密，建立和逐步引入保护信息的规范和法律基础，与欧洲标准和世界标准保持一致；
- 开发最新的信息保护方法，以全面完成保护电信网络信息的任务；
- 建立相关系统，在法律规定的情形下，合法拦截电信网络的信息；

- 建立公众信息和电信网络领域的国家协调中心，帮助建立国家和非政府中心，应对和处理这些网络出现的事故。

19. 乌克兰信息保护的规范和法律基础还包括以下方面的法令：有关国家安全基本原则的法令；有关信息的法令；有关信息保护和信息与电信系统的法令；总统和内阁关于对乌克兰的信息进行技术保护的指令；保护信息和电信系统及网络的规则以及与国际数据传输网络连接的程序等。它还包括司法部登记的许多规范性法令(其目的在于管理信息系统与全球信息传输网络的连接)、特定类型的活动的许可证制度以及评估信息保护的程序。

20. 规范性法令规定，要对信息实行所需的保护，就必须采用受保护的信息和通信技术系统，也就是必须整合全面信息保护系统，作为立法和后勤措施、软件和硬件的单一整体，用以对抗威胁。这一综合系统及其信息保护组成部分必须获得认证，必须符合信息保护的标准。

21. 为了管理全面信息保护系统及其组成部分的要求，乌克兰拟定和引入了五十多套技术标准，为信息保护的评估、信息和通信技术的分类、实现信息保护的程序、对全面信息保护系统的单个组成部分的要求(视涉及的信息和通信技术、最终目的、使用领域和处理的信息类型而异)制定了标准。

22. 乌克兰还创建了本国评估信息技术安全的国家体系。该体系基于一套防止信息和电信系统的信息遭受未经许可的利用的管理文书；这些文书已与欧洲联盟国家的类似文书和国际标准(特别是国际标准组织/国际电工委员会的 15408 号标准)实现了统一。

23. 此外，乌克兰还正在建立本国的组织和技术措施体系，以期防止对国家当局、执法部门、海关和税务当局、信贷与金融机构及其他部门的信息与电信系统实施未经授权的行为，特别是通过因特网干扰其工作的企图。

24. 国际社会为了应对此类行为，设立了分布广泛的高级系统(计算机应急小组)，负责对危及信息资源安全的事故作出快速反应。称为“事故反应和安全小组论坛”的国际组织在国际一级协调这些小组的行动。

25. 为确立此类行为的法律和监管基础，乌克兰国家特别通信与信息保护局的管理层于 2008 年 6 月 10 日颁布了第 94 号令，核准了中央和地方政府、军事单位、公司、机构和组织之间开展协调的程序(无论所有权形式如何)，以防止、侦测和处理针对信息和通信系统中的国家信息资源实施的未经授权的行为之后果。

26. 为实施这一指令，还设立了有关的网站和电子邮件地址(www.cert.gov.ua)。

27. 乌克兰借鉴了国际上在确保信息资源安全方面的经验，正在采取措施在国家特别通信与信息保护局内部设立一个国家协调员的职位，负责防止信息和电信系统的信息安全受到侵犯(乌克兰计算机应急小组)。该职位的任职者将获得“事故

反应和安全小组论坛”的认可。在这方面，国家特别通信与信息保护局的管理层代表曾于 2009 年 3 月 17 日与芬兰通信管理局的一名信息安全高级顾问举行了会晤。

28. 在 2006 年至 2008 年期间，尽管乌克兰计算机应急小组当时还不是“事故反应和安全小组论坛”的认可成员，乌克兰还是从芬兰、澳大利亚、奥地利、斯洛文尼亚和其他国家的计算机应急小组收到了 200 多起有关乌克兰因特网用户实施未经授权行为的报告。这促使有关当局向相关的因特网服务提供者发送了 250 多封电子邮件，以确定有害软件和病毒的来源地。另外，乌克兰还在 2007 年 5 月采取行动防止从乌克兰境内发起的、针对爱沙尼亚服务器的“分布式拒绝服务攻击”(DDoS)，并在 2007 年 10 月阻止了一起针对乌克兰总统官方网站的分布式拒绝服务攻击。

29. 值得补充的是，乌克兰还建立了法律和监管框架，并努力确保国家特别通信与信息保护局与执法机构之间的合作，以期实施措施保护信息与电信系统的国家信息资源的安全，提高系统应对未经授权侵犯此类信息资源的行为的有效性。

30. 因此，乌克兰如今可以在建立信息与电信系统以及在这些系统内建立全面信息保护系统的所有阶段对信息予以保护，无论处理的信息的类型和重要性如何，也无论信息与电信系统的类型和复杂程度如何。此外，乌克兰对整个信息与电信系统的信息资源保护的要求、设计、开发、安全与评估的所有基本考察办法，都与联合国会员国及欧洲联盟成员国的国家安全部门所采用的方法保持一致。

31. 为了培训信息安全与计算机工程领域的专家，乌克兰还设立了一个信息保护研究所，作为国立信息与通信技术大学的一个学术与科学部门。