

保护上网儿童政策 制定者指南

2020



保护上网儿童政策制定者指南

2020

致谢

本指南由国际电信联盟（国际电联）与活跃在信息通信技术（ICT）行业以及保护（上网）儿童领域的主要机构一些撰稿人组成的工作组制定，其中包括以下组织：

国际终止儿童卖淫及贩卖儿童协会（ECPAT International）、全球上网儿童网络、终止暴力侵害儿童行为全球伙伴关系、HABLATAM项目、更安全的互联网中心的Insafe网络、国际刑警组织、国际失踪和被剥削儿童中心、国际残疾人联盟、国际电信联盟（ITU）、网络观察基金会（IWF）、伦敦经济学院、负责暴力侵害儿童问题的秘书长特别代表办公室和有关买卖儿童和儿童性剥削问题的特别报告人、Privately SA、RNW媒体、英国更安全的互联网中心、WeProtect全球联盟（WPGA）和世界儿童基金会。

该工作组由David Wright（英国更安全的互联网中心/SWGfL）担任主席，由Fanny Rotino（国际电联）进行协调。

如果没有撰稿人投入的时间、热情和奉献精神，这些指南则不可能问世。欧洲COFACE-家庭协会、澳大利亚电子安全专员、欧盟委员会、电子世界集团公司（e-WWG）、经合发展组织（OECD）、哈佛大学青年与媒体/伯克曼-克莱因互联网与社会中心以及各国政府和私营部门利益攸关方也都做出了宝贵的贡献，它们的共同目标是为儿童和青少年打造更好、更安全的互联网。

对于贡献了宝贵时间和见解的下述合作伙伴，国际电联表示衷心感谢（按照合作伙伴所属单位的英文名称字母排序）：

- Martin Schmalzried（欧洲COFACE-家庭协会）
- Livia Stoica（欧盟理事会）
- John Carr（国际终止儿童色情业及贩卖儿童协会）
- Julia Fossi和Ella Serry（澳大利亚电子安全专员）
- Manuela Marta（欧盟委员会）
- Salma Abbasi（电子世界集团公司）
- Amy Crocker和Serena Tommasino（终止暴力侵害儿童行为全球伙伴关系）
- Lionel Brossi（HABLATAM）
- Sandra Marchenko（国际失踪与被剥削儿童中心）
- Karl Hopwood（Insafe）¹

¹ 在“连通欧洲机制（CEF）”下，欧洲学校网（European Schoolnet）代表欧盟委员会管理“让孩子们用上更好的互联网”平台，其中包括协调欧洲互联网安全中心网络Insafe网络。更多信息请访问：www.betterinternetforkids.eu。

- Lucy Richardson（国际残疾人联盟）
- Matthew Dompier（国际刑警组织）
- Fanny Rotino（国际电联）
- Tess Leyland（IWF）
- Sonia Livingstone（伦敦政治经济学院和“全球上网儿童”）
- Elettra Ronchi（OECD）
- Manus De Barra（负责暴力侵害儿童问题的秘书长特别代表办公室）
- Deepak Tewari（Privately SA）
- Pavithra Ram（RNW媒体）
- Maud De Boer-Buquicchio（联合国有关买卖儿童和儿童性剥削问题的特别报告人）
- David Wright（英国更安全的互联网中心/SWGfL）
- Iain Drennan和Susannah Richmond（WeProtect全球联盟）
- Lina Fernandez和Joanna Rubinstein博士（美国世界儿童基金会）
- Sandra Cortesi（青年与媒体）

ISBN

978-92-61-30125-5（纸质版）

978-92-61-30455-3（电子版）

978-92-61-30115-6（EPUB版）

978-92-61-30465-2（Mobi版）



打印本报告之前，请考虑到环境影响

© ITU 2020

一些保留的权利。该作品通过创作共享署名-非商业-共享3.0 IGO许可（CC BY-NC-SA 3.0 IGO）向公众授权。

根据本许可证的条款，如果作品被适当引用，您可以出于非商业目的复制、重新分发和改编作品。在使用该作品时，不应建议国际电联认可任何具体的组织、产品或服务。不允许未经授权使用国际电联的名称或标志。如果您改编作品，那么您必须在相同或等效的创作共用许可下使您的作品获得许可。如果您创作了这部作品的译文，你应该加上下面的免责声明以及建议的引文：“这部译文不是由国际电信联盟（ITU）创作的。国际电联对本译文的内容或准确性不承担任何责任。英文原版应为具有约束力的真实版本”。欲了解更多信息，请访问：<https://creativecommons.org/licenses/by-nc-sa/3.0/igo/>。

前言

在互联网几乎渗透到现代生活各个方面的世界里，让青少年用户安全上网已经成为每个国家越来越迫切的问题。

早在2009年国际电联就制定了第一套《保护上网儿童指南》。自那时以来，互联网的发展已超越了所有人的认知。它已成为儿童娱乐和学习更加丰富的无限资源库。与此同时，当孩子们在无人陪伴的情况下上网时，互联网也已成为险象环生之处。

从隐私问题到暴力和不适当的内容、网上的骗子，以及网上的性诱骗、性虐待和性剥削的等等，儿童面临着林林总总的风险。威胁在不断增加，罪犯越来越多地同时在许多不同的法律管辖区活动，限制了针对具体国家的应对和补救措施的有效性。

此外，在新冠病毒疫情全球大流行的情况下，首次进入网络世界的儿童人数激增，在网上继续他们的学习和保持社交活动。为防止病毒而实施的隔离措施不仅意味着许多年幼的儿童比他们的父母可能计划的时间更早开始网上互动，而且由于许多父母需要兼顾工作，因此无法监督他们的孩子，使青少年有可能接触到不适当的内容或成为犯罪分子进行儿童性虐待犯罪的目标。

与以往任何时候相比，保护上网儿童安全都需要国际协作和协调的应对措施，这需要众多利益攸关方的积极参与和支持 – 从包括私营部门平台、服务提供商和网络运营商在内的行业利益攸关方，到政府和民间团体。

认识到这一点，国际电联成员国于2018年要求我们不仅要像过去那样对《保护上网儿童指南》及时地定期进行更新。而且对指南的这些新的修订要从头开始重新思考、重新编写和重新设计，以反映出儿童所处数字化环境的重大转变。

除了应对数字技术和平台的新发展外，新版指南还填补了一项重要的空白：残疾儿童所面临的情况，网络世界为他们提供了一条特别重要的生命线，使他们能够充分地、充实地参与社会。本书还考虑到了移民儿童和其他弱势群体的特殊需要。

对政策制定者来说，我们希望这些指南将成为一个坚实的基础，在此基础上制定包容性、利益攸关多方的国家战略，包括与儿童进行公开磋商和对话，以制定更有针对性的措施和更有效的行动。

在制定这些新准则的过程中，国际电联及其合作伙伴寻求创建一个高度可用、灵活且适应性强的框架，该框架牢牢建立在国际标准和共同目标 – 尤其是《儿童权利公约》和联合国可持续发展目标 – 的基础上。本着国际电联作为全球召集者的精神，我感到自豪的是，这些经修订的指南是全球合作努力的产物，由来自广泛的多利益攸关方团体的国际专家共同撰写。

我还很高兴地向大家介绍我们新的保护上网儿童的吉祥物Sango（桑哥），这是一个友善、勇敢和无畏的角色，完全是由许多儿童一起设计的，这个吉祥物是国际电联新的国际青年人推广计划中的组成部分。

在这个越来越多青少年开始上网的时代，这些保护上网儿童的指南比以往任何时候都更加重要。政策制定者、业界、父母和教育工作者以及儿童本身，都将发挥着重要作用。我一如既往地感谢你们的支持，我期待着在这个关键问题上继续我们的密切合作。



电信发展局主任
多琳·伯格丹-马丁

序言

三十年前，几乎所有政府都承诺尊重、保护和促进儿童权利。《联合国儿童权利公约》（CRC）是历史上得到最广泛批准的国际人权条约。虽然过去三十年取得了显著进展，但仍然存在重大挑战，儿童面临的新风险领域层出不穷。

2015年，所有国家都根据《2030议程》和17项普遍可持续发展目标（SDG）重申了对儿童的承诺。例如，目标16.2呼吁到2030年结束对儿童的虐待、剥削和一切形式的暴力和酷刑。但是保护儿童是17个可持续发展目标中11个目标的共同主线。如图1所示，联合国儿童基金会（UNICEF）将儿童置《2030年议程》的中心。

图1：儿童、ICT和SDG



《2030可持续发展议程》承认ICT可以成为实现SDG的关键驱动因素。信息通信技术（ICT）的推广和全球互连具有加速人类进步、弥合数字鸿沟和建设知识社会方面的潜力。议程进一步确定了在教育（目标4）、性别平等（目标5）、基础设施（目标9—普及和负担得起的互联网接入）和目标17—伙伴关系和实施手段¹中使用ICT促进可持续发展的具体目标。ICT作为实现17项可持续发展目标中每一项目标的驱动力，有能力深刻改变整个经济。ICT已经通过赋予全球数十亿人享用教育资源和医疗保健，以及电子政务和社交媒体等服务的能力取得了长足进步。为了降低数字世界的风险，同时让更多的儿童和年轻人从中受益，各国政府、民间社会、地方社区、国际组织和行业必须同心协力。为了实现保护儿童上网安全的国际目标，尤其需要政策制定者。为了应对信息和通信技术的快速发展带来的挑战及其带来的儿童保护挑战，国际电信联盟（国际电联）于2008年11月发起了儿童在线保护倡议，这是一项多利益攸关方的国际倡议。

信息通信技术的普及为儿童和青年就影响其生活和社区的问题进行交流、联系、分享、学习、获取信息和表达意见创造了前所未有的机会。

¹ UNDP, 可持续发展目标 | UNDP, undp.org, 访问于2020年1月29日, <https://www.undp.org/content/undp/en/home/sustainable-development-goals.html>; 赵厚麟《信息通信技术为何对于实现可持续发展目标至关重要》, 国际电联, 第48期《国际电联新闻》杂志, 访问于2020年1月29日, https://www.itu.int/en/itu-news/Documents/2017/2017-03/2017_ITUNews03-en.pdf。

但更广泛、更容易获得的互联网和移动技术也对儿童的安全和福祉构成了重大挑战 – 无论在线还是离线。

为了降低数字世界的风险，同时让更多的儿童和年轻人从中受益，各国政府、民间社会、地方社区、国际组织和业界必须同心协力。为了实现保护儿童上网安全的国际目标，尤其需要政策制定者。

为了应对ICT快速发展带来的挑战及其带来的儿童保护挑战，国际电信联盟（ITU）于2008年11月推出**保护上网儿童（COP）举措**，作为一项利益攸关多方的国际举措，保护弱者，尤其是儿童（18岁以下互联网使用者占三分之一）。作为WSIS C5行动方面（树立使用ICT的信心并提高安全性）的唯一推进方，国际电联在全球范围内通过利益攸关多方为保护上网儿童付出艰辛的努力。该举措旨在将全球社会各行各业的合作伙伴团聚起来，为世界各地的儿童打造安全的上网体验并提高他们的能力。

此外，2018年在迪拜举行的国际电信联盟全权代表大会重申了COP的重要性，承认该举措是提高认识、分享最佳做法以及在制定和执行COP路线图方面向成员国，特别是发展中国家提供帮助和支持的平台。大会还认识到在《联合国儿童权利公约》和其他人权条约框架内保护上网儿童的重要性，鼓励参与保护上网儿童的所有利益攸关方开展合作。

大会认识到《2030可持续发展议程》，该议程在可持续发展目标中涉及保护上网儿童的各个方面，特别是可持续发展目标1、3、4、5、9、10和16；大会还认识到关于残疾人 and 有特殊需要的人无障碍获取电信/ICT的**第175号决议（2018年，迪拜，修订版）**和世界经济大会（WTDC）关于ITU-D在保护上网儿童中的作用的**第67号决议（2017年，布宜诺斯艾利斯，修订版）**。

2019年末，国际电联/教科文组织（UNESCO）宽带可持续发展委员会发布了《**儿童在线安全报告**》，其中包含关于如何为儿童打造更安全的互联网的可行建议。

2009年，国际电联围绕**COP举措**发布了第一套保护上网儿童指南。在过去十年里，COP指南已被翻译成多种语言，并被世界上许多国家用作有关保护上网儿童的路线图和国家战略参考文献。这些指南为国家政府实体、民间社会组织、儿童保育机构、行业和许多其他利益攸关方进行的保护上网儿童工作做出贡献。

更具体地说，在许多成员国，如非洲区域的喀麦隆、加蓬、冈比亚、加纳、肯尼亚、塞拉利昂、乌干达和赞比亚，阿拉伯区域的巴林和阿曼；亚太地区的文莱、柬埔寨、基里巴斯、印度尼西亚、马来西亚、缅甸和瓦努阿图；以及欧洲地区的波斯尼亚、格鲁吉亚、摩尔多瓦、黑山、波兰和乌克兰，指南已用于起草、制定和实施国家保护上网儿童战略。

此外，这些指南为区域性活动奠定了基础，如保护上网儿童区域性大会（ACOP）：增强未来数字公民的权能（2014年，乌干达坎帕拉）以及东盟保护上网儿童区域性大会（2020年，泰国曼谷）。

根据**第179号决议（2018年，迪拜，修订版）**，国际电联被责成与COP举措合作伙伴和利益攸关方合作更新四套指南，同时考虑到电信行业的技术发展，包括关于残疾儿童和有特殊需求儿童的指南。

通过这一进程，专家和相关利益攸关方对这些指南进行了大刀阔斧的更新和认真的审议，确立了一系列广泛的建议，以确保儿童在数字世界中的安全。这些建议是利益攸关多方合作努力的结果，利用了世界各地许多组织和个人在保护上网儿童领域的知识、经验和专长。他们的目的是为后代建立一个安全的网络世界。指南旨在发挥蓝图的作用，以符合国家或地方习俗和法律的方式予以调整和使用。此外，这些指南涉及影响所有18岁以下儿童和青少年的问题，承认每个年龄组的不同需求。指南还旨在满足不同生活条件下的儿童以及有特殊需求和残疾儿童的需求。指南还强化了保护上网儿童的范围，探讨儿童在网上可能遇到的所有风险、威胁和伤害，并在这些风险、威胁和伤害与数字世界可能给儿童生活带来的好处之间保持谨慎的平衡。

希望指南不但能带来一个更为包容的信息社会的创建，而且还能促进成员国履行其保护和实现儿童权利的义务。这些权利在联合国大会1989年11月20日第44/25号决议通过的联合国《儿童权利公约》²和信息社会高峰会议³（WSIS）成果文件中做了规定。

通过发布这些指南，保护上网儿童（COP）举措号召所有利益攸关方推动实施政策和战略，保护儿童在网络空间的安全，推动儿童更安全地访问所有在线资源能提供的绝佳机会。

² UNICEF，《儿童权利公约》，[unicef.org](https://www.unicef.org/child-rights-convention)，访问于2020年1月29日，<https://www.unicef.org/child-rights-convention>。

³ WSIS分两个阶段举行：日内瓦（2003年12月10-12日）和突尼斯（2005年11月16-18日）。WSIS结束时勇敢做出承诺：“建设一个以人为本、具有包容性和面向发展的信息社会。在此信息社会中，人人可以创造、获取、使用和分享信息和知识。”

致谢	ii
前言	iv
序言	vi
1 文件综述	1
1.1 目的	1
1.2 范围	1
1.3 总体原则	2
1.4 这些指南的使用	2
2 引言	4
2.1 保护上网儿童何意?	5
2.2 数字世界中的儿童	6
2.3 技术对儿童数字体验的影响	8
2.4 在线儿童面临的主要威胁	9
2.5 在线儿童面临的主要危害	11
2.6 脆弱的儿童	16
2.7 儿童对在线风险的看法	18
3 为制定国家保护上网儿童战略做好准备	20
3.1 参与方和利益攸关方	20
3.2 保护上网儿童方面的现有响应机制	24
3.3 应对网上伤害示例	27
3.4 国家保护上网儿童战略的益处	27
4 关于框架和实施的建议	29
4.1 有关框架的建议	29
4.1.1 法律框架	29
4.1.2 政策和制度框架	30
4.1.3 监管框架	30
4.2 有关实施的建议	31
4.2.1 性剥削	32
4.2.2 教育	33
4.2.3 业界	33
5 制定国家保护上网儿童战略	35

5.1	国家战略要素清单	35
5.2	问题示例	42
6	参考资料	43
	附录1: 术语	47
	附录2: 针对儿童和青少年的接触犯罪	53
	附录3: WeProtect全球联盟	54
	附录4: 网上伤害响应示例	56

表、图、框列表

表目录

表1: 需要考虑的关键领域	35
---------------	----

图目录

图1: 儿童、ICT和SDG	vi
图2: 儿童面临的在线威胁分类	9

框目录

上网	7
互联网的使用	7
危害	11

1 文件综述

1.1 目的

国家政府有义务在“真实”世界和“虚拟”世界中为儿童提供保护。这很重要，由于新技术现在已经以诸多重要方式全面溶入众多儿童和青少年的生活中，因此不应再对“真实世界”事件与网络事件之间的差别做严格区分。二者之间正日益交织在一起，变得越来越相互依存。

政策指定者¹和所有其他相关利益攸关方都可以发挥非常重要的作用。技术发展的速度意味着许多传统的决策方法不再适合这个目的。政策制定者需要制定一个具有适应性、包容性、适合快速变化的数字时代的法律框架，以保护上网儿童。

这些指南的目的是为国际电联成员国的政策制定者提供一个方便用户和灵活的框架，以理解他们的法律义务并采取行动，在现实、物理和虚拟世界中为儿童提供保护。

指南通过向政策制定者提出若干重要问题实现这一目标：

- 1) 什么是保护上网儿童？
- 2) 作为政策制定者，我为什么需要关心儿童在线保护？
- 3) 我国的法律、社会政治和发展背景是什么？
- 4) 政策制定者应如何开始考虑和制定本国有效和可持续的儿童在线保护政策？

在此过程中，这些指南利用现有的模型、框架和资源，提供有关世界各地良好做法的背景和见解。

1.2 范围

儿童在线保护的范围扩大到儿童在线受到的任何伤害，涵盖威胁儿童安全和福祉的广泛风险。这是一个复杂的挑战，必须从多个角度予以应对，包括立法、治理、教育、政策和社会。

此外，儿童在线保护必须基于对数字环境中儿童面临的一般和特定国家风险、威胁和伤害的理解。这需要有明确的定义和明确的干预参数，包括并区分构成犯罪的行为和虽不违法但对儿童福祉构成威胁的行为。

为此，指南概述了数字环境中儿童当前面临的威胁和危害。然而，技术及其相关威胁和危害的发展速度意味着传统的决策速度和方法无法与时俱进。数字时代的政策制定者需要建立具有适应性和包容性的法律和政策框架，以应对现有的挑战，并尽可能预测未来的挑战。要做到这一点，需要与每个利益攸关方合作，包括ICT行业、研究界、民间团体、公众和儿童本身。考虑儿童在线保护的总体原则可以对这一进程提供支持。

¹ 政策制定者一词指负责制定和实施政策的所有利益攸关方，特别是政府内部各方。

1.3 总体原则

这里列出的十一项整合原则通过综合利用将有助于制定一项前瞻性和全面的国家儿童在线保护战略。

这些原则的顺序反映了一种逻辑性叙述，而不是重要性顺序。

儿童在线保护战略应：

- 1) 基于包含政府、行业和社会在内的整体愿景；
- 2) 是对整个数字环境的全面理解和分析的结果，但要适合国家的情况和优先事项；
- 3) 尊重并符合《联合国儿童权利公约》和其他主要国际公约和法律中规定的儿童基本权利；
- 4) 尊重并符合现有的、类似的和相关的国内法律和战略，如虐待儿童法或儿童安全战略；
- 5) 尊重儿童的公民权利和自由，不应为了保护而牺牲这些权利和自由；
- 6) 在包括儿童在内的所有相关利益攸关方的积极参与下制定，论述他们的需求和责任，满足少数群体和边缘化群体的需求；
- 7) 旨在与更广泛的政府经济和社会繁荣计划保持一致，并使ICT对可持续发展和社会包容做出最大的贡献；
- 8) 考虑到国家的具体情况，利用现有最适当的政策手段实现其目标；
- 9) 设在政府的最高一级，负责分配相关的角色和责任，并分配足够的人力和财政资源；
- 10) 帮助建立一个儿童、父母/看护人员和利益攸关方可以信任的数字环境；
- 11) 引导利益攸关方努力增强儿童的能力，并对他们进行数字扫盲教育，以保护他们在网上的权益。

1.4 这些指南的使用

这些指南考虑了相关研究、现有模式和材料，并为制定国家儿童在线保护战略提出了明确的建议。

- 第2节介绍了儿童在线保护，并深入分析了最近的研究，包括新兴技术、对儿童的主要威胁和危害。
- 第3节阐述了如何拟定国家儿童在线保护战略，包括相关利益攸关方、应对在线威胁和伤害的现有示例以及制定国家战略的好处。

- 第4节涵盖框架和实施的建议。
- 第5节概括了制定国家儿童在线保护战略的国家核对清单。
- 第6节给出了有用的参考资料。

2 引言

2019年，超过一半的世界人口使用互联网。最大的用户群体年龄在44岁以下，16至24岁和35至44岁的使用率同样高。在全球范围内，三分之一的儿童使用互联网（0-18岁）²。在发展中国家，儿童和年轻人正在引领互联网的使用³，据估计，在未来五年，这一人口将增加一倍以上。新一代人是随着互联网成长起来的，大多数人都在使用移动网络技术，尤其是在南部地球⁴。

虽然互联网接入对实现儿童权利至关重要，但在接入方面仍然存在显著的区域、国家、性别和其他差异，限制了女孩、残疾儿童、少数民族儿童和其他弱势群体的机会。就数字性别差距而言，研究表明，除美国外，在每个区域，男性互联网用户大大超过女性用户。在许多国家，女孩没有与男孩相同的上网机会，即使有，女孩不仅在更大程度上受到互联网使用的监控和限制，而且在上网过程中，她们也可能发现自己的安全受到威胁⁵。很明显，缺乏数字技能或说少数民族语言的儿童和年轻人无法在网上轻松找到相关内容，来自农村地区的儿童数字技能较少，上网时间较长（尤其是玩游戏），并且较少接受父母的调解和监督⁶。

然而，如果不承认数字技术在提供丰富多彩的内容和和赋能方面的作用，无法进行任何关于风险和威胁的对话。互联网和数字技术已经为交流、游戏、欣赏音乐和从事各种文化、教育和技能提升活动开辟了许多新的途径。互联网可以为获得保健和教育服务提供必不可少的途径，并提供对年轻人而言既重要但在他们的圈子中视为禁忌的话题的信息。

正如儿童和年轻人经常站在采用和适应互联网提供的新的可能性的最前沿一样，他们也面临一系列与安全和福利有关的问题，这些问题必须得到社会的承认和正视。在网上公开讨论儿童和年轻人面临的风险至关重要。讨论打开了一个平台。在这个平台上，可以教会儿童和年轻人如何识别风险，如何预防或应对可能出现的危害，以及互联网可以提供的优势和机会。

² 经合发组织（OECD），《新技术和21世纪的儿童：最近的趋势和成果》，OECD第179号教育工作文稿（OECD教育和技能总局），访问于2020年1月27日，<https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=EDU/WKP%282018%2915&docLanguage=En>。

³ 英国通信管理局（Ofcom），《儿童和家长：2018年媒体的使用和态度报告》（Ofcom），访问于2020年1月27日，https://www.ofcom.org.uk/_data/assets/pdf_file/0024/134907/children-and-parents-media-use-and-attitudes-2018.pdf。

⁴ 国际电联，《衡量信息社会报告》，访问于2020年1月16日，https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2018-SUM-PDF-E.pdf。

⁵ 《青年与数字媒体：地中海收入国家的使用、风险和机遇》，GAGE，访问于2020年1月29日，2020，<https://www.gage.odi.org/publication/digital-media-risks-opportunities/>。

⁶ Livingstone, S.、Kardefelt Winther D.和Hussein, M.（2019年），《全球儿童在线比较报告》- Innocenti 研究报告（UNICEF研究办公室- Innocenti（佛罗伦萨））<https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html>。这可能会产生意想不到的结果，例如，Hablatam在五个拉丁美洲国家开展的研究表明，在弱势群体中，儿童可能会利用约会平台、视频游戏和社交网络进行非法的金钱交易。Contactados al Sur network- “Hablatam,” Hablatam 2020年项目，访问于2020年2月6日，<https://hablatam.net/>。

在世界许多地方，年轻人对他们在网上面临的一些风险有很好的理解⁷⁸。例如，研究表明，大多数儿童和年轻人能够区分网络欺凌和网上开玩笑或戏弄。他们认识到网络欺凌具有公共性，其目的是伤害他人，然而平衡儿童的网络机会和风险仍然是一个挑战⁹。

对国际电联成员国而言，保护上网儿童和青年人仍然是一个优先事项，必须与促进儿童和青年人在线机会的努力保持谨慎平衡¹⁰，而且必须以保护儿童和青年人的方式进行，而不影响他们或广大公众获得信息，或享有言论、表达和结社自由的能力。

要解决儿童和年轻人面临的风险显然需要专项投资和具有创造性的解决方案，尤其是因为，儿童和成人之间的数字鸿沟限制了父母、教师和监护人的指导。与此同时，随着儿童和青年长大成人、成为父母和社会的积极成员，他们有潜力和不容错过的缩小数字鸿沟的机会。

有鉴于此，在互联网上建立信任必须是公共政策的首要 and 核心。政府和社会需要与儿童和年轻人合作，了解他们的观点，并引发关于风险和机遇的真正公开辩论。为儿童和年轻人管理网上风险提供支持可能是有效的，但政府也必须确保为那些在网上遭受伤害的人提供足够的支持服务，并确保儿童知道如何获得这些服务。

一些国家难以分配足够的资源以解决在线儿童的数字扫盲和安全问题。然而，儿童报告说，家长、教师、技术公司和政府在开发支持他们在线安全的解决方案中发挥着重要作用。国际电联成员国还表示，大力支持加强知识共享和协调努力，以确保更多在线儿童的安全⁹。

儿童和年轻人正在日益复杂的数字环境中探索，将人工智能用于机器学习、大数据分析、机器人、虚拟和增强现实以及物联网将改变儿童的媒体实践。就像今天一样，需要为未来的孩子、父母和社区制定政策并进行投资。

2.1 保护上网儿童何意？

网络技术为儿童和青年相互交流、学习新技能、发挥创造性以及为全人类建设更美好的社会提供了很多可能性，但网络也常常导致新的风险，例如使他们面临诸如隐私、非法内容、骚扰、网络欺凌、个人数据滥用或性诱骗，甚至儿童性虐待。

这些指南为进行数字扫盲的儿童和年轻人应对在网上可能遇到的所有潜在威胁和伤害制定了一个整体方法。他们认识到，所有相关的利益攸关方都在数字复原力、福祉和保护方面发挥作用，同时受益于互联网提供的机会。

保护儿童和青年是一项共同的责任，所有利益攸关方都有责任确保所有人的可持续未来。要做到这一点，政策制定者、行业、父母、看护人员、教育者和其他利益攸关方必须确保儿童和年轻人能够发挥他们的潜力，无论在线和离线。

⁷ 自2016年以来，国际电联在COP范畴内就网络欺凌、数字扫盲和儿童在线活动等相关问题与儿童和成人利益攸关方进行了磋商。

⁸ 国际电联青年磋商：<https://www.itu.int/en/council/cwg-cop/Pages/meetings.aspx>。

⁹ UNICEF，《全球儿童在线比较报告》（2019年）。

¹⁰ 国际电联，《庆祝“保护上网儿童”推出十周年》，《国际电联新闻》，2018年2月6日，<https://news.itu.int/celebrating-10-years-child-online-protection/>。

虽然没有关于儿童在线保护的普遍定义，但它旨在采取全面的方式，为儿童和青年人建立安全、适龄、包容性和参与性的数字空间，其特点包括：

- 面对威胁时的反应、支持和自助；
- 防止伤害；
- 确保保护儿童和为儿童提供成为数字公民的机会之间的动态平衡；
- 维护儿童和社会两方面的权利和责任。

此外，由于技术和社会的快速进步以及互联网的无国界性质，儿童在线保护需要具有灵活性和适应性以便行之有效。虽然这些指南有助于深入了解儿童和青少年在网上面临的主要风险，包括有害和非法内容、骚扰、网络欺凌、滥用个人数据或性欺诈以及儿童性虐待和性剥削，但随着技术创新的发展，新的挑战将会出现，而且通常会因地区而异。然而，应对新挑战的最佳方式是全球社会的共同努力，因为，应对这些挑战需要找到新的解决方案。

2.2 数字世界中的儿童

互联网改变了我们的生活方式。它完全融入了儿童和年轻人的生活，因此不可能将数字世界和物理世界分开来考虑。今天，三分之一的互联网用户是儿童和年轻人，联合国儿基会估计，已有71%的年轻人上网。

这种连接使人们的能力得到显著提高。网络世界让儿童和年轻人克服劣势和残疾，并为娱乐、教育、参与和建立关系提供了新的舞台。如今，数字平台被用于各种活动，并且通常是多媒体体验。

获得并学会使用和探寻这一技术被视为年轻人发展的关键要素，而且，他们从很小的时候就开始涉足。政策制定者必须明白，儿童和年轻人往往在达到规定的最低年龄之前就开始使用平台和服务，因此，教育必须尽早开始。

儿童和年轻人希望参与到对话中来，他们作为“数字原生代”拥有可以分享的宝贵专业知识。政策制定者和从业者必须让儿童和年轻人参与一直进行的关于在线环境的辩论，以支持他们的权利。

上网

2019年，世界一半以上的人口使用互联网（53.6%），据估计有41亿用户。在全球范围内，三分之一的互联网用户是18岁以下的儿童¹。在一些低收入国家，这一比例上升到约二分之一，而在高收入国家，这一比例约为五分之一。根据联合国儿童基金会的数据，全世界71%的年轻人已经上网²。因此，儿童和年轻人现在是互联网上一股重要、长期和持久的力量³。互联网服务于其他社会、经济或政治目的，已经成为家庭或消费产品或服务，是家庭、儿童和年轻人生活方式的组成部分。

2017年，从区域来看，儿童和年轻人上网与收入水平高度相关。低收入国家的儿童互联网用户往往比高收入国家少。

大多数国家的儿童和年轻人周末上网的时间比工作日多，青少年（15-17岁）上网时间最长，视国家情况，平均为2.5-5.3小时。

互联网的使用

在儿童和年轻人中，最受欢迎的上网设备是手机，其次是台式电脑和笔记本电脑。儿童和年轻人在一周内平均每天花大约两个小时上网，周末每天大约花两倍的时间。有些人感觉永远保持连接，但是许多其他人仍然无法在家里上网。

实际上，大多数使用互联网的儿童和年轻人通过不止一个设备访问互联网：至少每周连接一次的儿童和年轻人有时会使用多达三种不同的设备。在接受调查的每个国家，年龄较大的儿童和富裕国家的儿童通常使用更多的设备，而男孩使用的设备比女孩略多。

无论对女孩还是男孩来说，最受欢迎的活动是观看视频剪辑。超过四分之三的使用互联网的儿童和年轻人表示，他们至少每周都在网上观看视频，或自己单独观看，或与家人一起观看。许多儿童和年轻人可以被认为是“积极的社交者”，他们使用几个社交媒体平台，如脸书、推特、互动游戏或Instagram。

儿童和年轻人也在网上参与政治，并通过博客发出自己的声音。

¹ Livingstone, S., Carr, J和Byrne, J. (2015年) 《三分之一：全球互联网治理在解决儿童权利方面的任务》，全球互联网管理委员会：论文系列，伦敦：CIGI and Chatham House, <https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights>。

² 宽带委员会，《儿童在线安全：最大限度地降低在线暴力、虐待和剥削的风险》（2019年），宽带可持续发展委员会，2019年10月第84号报告，https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf。

³ Livingstone, Carr和Byrne, 《三分之一：联网治理与儿童权利》。

参与网络游戏的总体水平因国家而异，大致与儿童和年轻人上网的情况一致，而10%至30%使用互联网的儿童和年轻人每周都参与创造性的在线活动。

出于教育目的，许多各种年龄的儿童和年轻人使用互联网做作业，甚至在缺课后补课或每周在网上寻找健康信息。年龄大的孩子似乎比年龄小的孩子对信息更有兴趣。

2.3 技术对儿童数字体验的影响

互联网和数字技术可以为儿童和年轻人提供机会，也带来风险。例如，当儿童使用社交媒体时，他们受益于许多探索、学习、交流和发展关键技能的机会。例如，社交网络被儿童视为平台，让他们在安全的环境中探索个人身份。拥有相关的技能并知道如何解决与隐私和名誉相关的问题对年轻人来说很重要。

一位14岁智利男孩表示：“我知道你在网上发布的所有东西都会永远留在网上，它会影响你未来的生活。”

然而，咨询显示，大多数儿童在13岁之前使用社交媒体¹¹，年龄核实服务普遍薄弱或缺乏，儿童面临的风险可能会加剧。当孩子们想要学习数字技能并成为数字公民，特别是关心他们的隐私时，他们倾向于把隐私与他们的朋友和熟人联系起来考虑。“我的朋友能看到什么？”——却不太考虑与陌生人和第三方的关系。再加上儿童天生的好奇心和通常较低的风险门槛，这可能使他们容易受到诱导、剥削、欺凌或与其他类型的有害内容接触。

通过移动应用进行图像和视频共享的广泛流行，尤其是儿童使用实时流媒体平台，带来了进一步的隐私和风险相关问题。一些孩子正在制作自己、朋友和兄弟姐妹的性图像，并在网上分享。对一些人来说，尤其是年龄较大的儿童，这可以被视为对性和性身份的自然探索，而对其他人来说，尤其是年龄较小的儿童，往往受到成人或其他儿童的胁迫。无论是哪种情况，由此产生的内容在许多国家都是非法的，可能会使儿童面临被起诉的风险，或者可能被用来进一步剥削儿童。

同样，网络游戏使孩子们能够实现他们玩游戏的基本权利，并建立联络，花时间和新朋友在一起，开发重要的技能。绝大多数情况下，这是积极的。然而，越来越多的证据表明，如果没有负责任的成年人的监督和支持，在线游戏平台也会给儿童带来风险，从游戏障碍、财务风险、儿童个人数据的收集和货币化，到网络欺凌、仇恨言论、暴力和暴露于不当行为或内容¹²，以及通过使用真实的、计算机生成的、甚至虚拟现实的图像和视频进行的网络诱骗，对儿童的性虐待和性剥削予以描述并使之常规化。

此外，技术的发展导致了物联网的出现，越来越多的设备能够通过互联网进行连接、通信和连网。这包括玩具、婴儿监视器和人工智能驱动的设备，这些设备可能会带来隐私和不必要的接触风险。

¹¹ Contactados al Sur network, “Hablatam”, UNICEF, 《全球儿童在线比较报告》（2019年）。

¹² UNICEF, 《全球儿童在线比较报告》（2019年）（2019年, UNICEF）。

2.4 在线儿童面临的主要威胁

成人和儿童在网上面临一系列风险和危险。然而，儿童是一个更加脆弱的群体。一些儿童也比其他儿童群体更容易受到伤害，例如残疾儿童¹³或流动儿童。政策制定者需要保证所有儿童都能在安全的数字环境中成长和接受教育。联合国《儿童权利公约》概括指出，儿童易受伤害，应保护他们免遭一切形式的剥削。

数字环境中的若干领域为儿童提供了巨大的机会，但同时也可能加剧风险，可能会严重伤害儿童并损害他们的福祉。成人和儿童都担心，例如，互联网可能被用来侵犯个人隐私，兜售虚假信息，或者更糟糕的是，允许访问色情内容。

在这里，区分风险和对儿童的伤害是至关重要的。并非所有可能带有风险因素的活动都是危险的，也并非所有的风险都必然对儿童有害，例如性短信，这是年轻人探索性和关系的一种方式，不一定有害。

图2：儿童面临的在线威胁分类¹⁴

	内容 儿童作为接收方 (大规模生产)	接触 儿童作为参与方 (成人发起的活动)	行为 儿童作为行为方 (肇事者/受害人)
攻击性	暴力/血腥内容	骚扰、跟踪	欺凌、恶意的同龄人活动
与性有关的	色情内容	“诱骗”、在与陌生人见面时性虐待	性骚扰、发送“色情信息”
价值观	种族主义/仇恨性内容	思想说服	可能有害的用户原创内容
商业	广告、嵌入式营销	个人数据利用和滥用	赌博、侵犯版权

来源：欧盟儿童在线（Livingstone, Haddon, Görzig和Ólafsson（2011年））

数字时代的到来给儿童保护带来了新的挑战。儿童必须获得安全地在网络世界中浏览并收获许多回报的能力。

政策制定者必须确保相关的立法、保障措施和工具到位，以使儿童能够安全地成长和学习。至关重要的是，儿童要具备识别威胁的必要技能，并充分理解他们在线行为的含义和细微差异。

在网上，儿童可能会遇到来自组织、成人和同龄人的大量威胁。

¹³ Lundy等人，《向前点击两次，向后点击一次》，《关于数字环境中残疾儿童的报告》（2019年10月，欧洲委员会），<https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f>

¹⁴ Livingstone, S., Haddon, L., Görzig, A和Ólafsson, K.（2011年），《互联网上的风险和安全：欧洲儿童的观点》，伦敦政经学院：全部发现，欧盟儿童在线，<http://eprints.lse.ac.uk/33731/>。

内容和操纵

- 接触不适当甚至犯罪内容会导致儿童走向极端，如自残、破坏性和暴力行为。接触此类内容同样会导致激进化或订阅种族主义或歧视性言论。众所周知，许多孩子不遵守网站上的年龄限制。
- 接触不准确或不完整的信息会限制儿童对周围世界的理解。基于用户行为定制内容的趋势会导致“过滤泡沫”，限制儿童开发和接触广泛的内容。
- 暴露于经过算法过滤并有意操纵的内容会极大地影响儿童的成长、意见、价值观和习惯。将儿童隔离在“回声室”或“过滤气泡”中，会阻止他们获取各种各样的观点和想法。

来自成人或同龄人的联系

儿童可能会遇到来自同龄人或成人的各种接触威胁。

- 在线欺凌比离线欺凌普及更广，传播速度更快。它可以发生在白天或晚上的任何时候，从而侵入以前的“安全空间”，并且可以匿名。
- 离线受害的儿童很可能在线受害。这使得残疾儿童在网上面临更高的风险，因为研究表明，残疾儿童更有可能遭受任何形式的虐待，特别是更有可能遭受性伤害。受害可能包括欺凌、骚扰、排斥和基于儿童实际或感知残疾的歧视，或基于与其残疾相关的方面，如他们的行为或说话方式，或他们使用的设备或服务。
- 诽谤和名誉损害：图像和视频可以被篡改并分享给数十亿人。判断错误的评论可以持续几十年，任何人都可以免费观看。
- 儿童可能通过互联网被本地或世界另一端的罪犯盯上、诱骗和虐待，他们声称的自己往往与事实不符。他们采取多种形式，包括激进化或胁迫发送自己的露骨性内容。
- 逼迫、欺骗或胁迫进行购买，无论是否得到付款人的许可。
- 推介性广告引发同意和销售数据的问题。

儿童的行为可能导致后果

- 在线欺凌尤其令人不安和具有破坏性，因为它可以更广泛地传播，具有更大程度的公开性，并且以电子方式传播的内容可以随时再现，这使得欺凌的受害者更难就此事件获得结案；它可能包含有害的视觉图像或伤人的话语；该内容一天24小时可用；电子手段的欺凌可能会全天候发生，因此它会侵犯受害者的隐私，即使是在本应“安全”的地方，比如他们的家；个人信息可以被操纵，视觉图像可以被篡改，然后被传递给其他人。此外，这些可以匿名进行。泄露个人信息会导致身体伤害的风险，包括现实生活中与网上熟人的接触，以及身体和/或性虐待的可能性。
- 未经许可剽窃和上传内容，包括未经许可拍摄和上传不妥照片，侵犯了他们自己或他人的权利。
- 侵犯他人的版权，例如下载应付费的音乐、电影或电视节目，因为这可对盗窃的受害者造成伤害。

- 强迫和过度使用互联网和/或在线游戏，损害对健康、树立信心、社会发展和总体福祉至关重要的社交和/或户外活动。
- 试图伤害、骚扰或欺负他人，包括假装他人（通常是另一个孩子）。
- 青少年越来越常见的行为是“性短信”（通过手机分享性图片或文本）。这些图片和文字经常在一段关系中的伙伴之间或与潜在的伙伴分享，但有时最终会被更广泛的受众分享。人们认为，青少年不太可能对这些行为的含义及其潜在风险有足够的理解。

2.5 在线儿童面临的主要危害

上一节提到了儿童在网上可能遇到的威胁。本节重点介绍这些威胁可能带来的危害。

危害

根据联合国儿童基金会关于互联网使用的研究，以下类别被视为风险和危害：

– 自我虐待和自我伤害：

- 自杀内容
- 歧视

– 接触不适当的材料：

- 接触极端/暴力/血腥内容
- 嵌入式营销
- 在线赌博

– 就此问题接受调查的儿童中，约有20%的人表示，在过去一年中，他们曾在网站或在线讨论中看到有人对自己进行身体伤害或自残。

– 激进化：

- 意识形态说服
- 仇恨言论

– 更多人报告儿童可能因为网上的仇恨言论或性内容、受到在线或离线伤害，或者与最初在网上遇到的人见面而感到不安。

– 性虐待和性剥削：

- 自行生成的内容

- 性诱骗
- 儿童性虐待材料（CSAM）
- 贩卖
- 旅行和旅游中对儿童的性剥削

2017年对丹麦、匈牙利和英国的儿童进行的一项研究发现，6%的儿童在未经允许的情况下分享了自己清晰的照片。

2019年，互联网观察基金会（IWF）发现132,000多个网页，确认其中包含儿童性虐待的图像和视频。每一个网页都可能包含从一张到数千张这种滥用的图片。

与网上暴力相关的风险，如未经同意传播裸照和性网络欺凌，体现出不平等的性别动态。女孩通常更容易受到针对性行为的性别压力的影响，经历更负面的后果并受到伤害。

— 侵犯和滥用个人数据：

- 黑客攻击
- 欺诈和盗窃

许多人对骗局和黑客很熟悉，但侵犯儿童在线活动的隐私被视为另一种侵权行为。成年人经常通过检查他们的手机和在线调查他们的活动来伤害年轻人。例如，来自巴西儿童的报告显示，来自不同年龄段的男孩和女孩都认为父母更多控制女孩使用互联网。试图对此进行的解释往往表明，在网上和网下互动的界限变得越来越模糊的情况下，女孩在某些情况下可能由于她们生活的社会结构而更加脆弱，特别是在她们的安全方面。

— 网络欺凌、跟踪和骚扰：敌对和暴力的同伴活动

聊天室和社交网站会为暴力和欺凌打开大门，因为匿名用户，包括年轻人，会进行攻击性或侮辱性的交流。在欧洲七个国家（比利时、丹麦、爱尔兰、意大利、葡萄牙、罗马尼亚和英国），Livingstone、Mascheroni、Ólafsson和Haddon¹发现，2010年平均有8%的儿童受到网络欺凌，而2014年有12%的儿童成为网络欺凌的受害者。

必须指出的是，弱势儿童往往面临更高的网络欺凌受害风险。

¹ Livingstone, S.、Mascheroni, G.、Ólafsson, K和Haddon, L.（2014年），《儿童的在线风险和机遇：来自欧盟在线儿童和网络儿童移动化的比较研究结果》，伦敦：伦敦政经学院，www.eukidsonline.net和<http://www.netchildrengomobile.eu/>。

聚焦：不平等加剧

2017年，非洲地区约60%的儿童没有上网，而欧洲只有4%。在世界各地，男性互联网用户超过女性用户，女孩使用互联网经常受到监控和限制。随着宽带扩展到世界上未相连的地区，这种不平等将显著增强¹⁵。

依赖手机而不是电脑的孩子可能只能获得次佳在线体验。说少数民族语言的儿童通常无法在网上找到相关内容，来自农村地区的儿童更有可能遭遇密码或金钱被盗的情况。

研究表明，世界各地的许多青少年必须克服网上参与的重大障碍。对许多人来说，接入挑战—连接不畅、数据和设备成本过高以及缺乏合适的设备—仍然是主要障碍。

随着价格可承受的宽带扩展到发展中国家，迫切需要采取措施，最大限度地减少这些儿童面临的风险和威胁，同时让他们能够享用数字世界的所有好处。

聚焦：儿童性虐待材料（CSAM）

问题的规模

互联网改变了CSAM制作、销售和供应的规模和性质。2018年，美国的科技公司报告了超过4500万的在线图像和视频，这些图像和视频被怀疑显示来自世界各地受到性虐待的儿童。这是一个全球性的行业，尽管人们努力阻止，但虐待的规模和严重程度与日俱增。

从历史上看，在一个离线的世界里，要找到CSAM需要违法者冒相当大的风险且花费巨大。有了互联网，违法者现在可以相对容易地获得这些材料，并卷入越来越危险的行为。相机体积更小，越来越多地融入我们生活的方方面面，使得制作CSAM和从非接触性虐待中获取内容的过程比以往任何时候都更加容易。

确定这个勾当和非法企业的确切规模或状况是不可能的。然而，很明显，现在流通的非法图像的数量可以数以百万计。几乎这些图像涉及的所有儿童都被复制了他们的图像。2018年，IWF追踪了一名已知在2013年获救的儿童的照片出现的频率。在三个月中，IWF分析师347次追踪到这些图像—每个工作日5次。

目前的格局

每当一个被虐待的孩子的图像出现并反复出现在网上，或者被违法者下载，这个孩子就被再次虐待。受害者被迫在余生中忍受这些图像的长期存在和流传。

一旦描述儿童性虐待的材料或宿主网页被发现，尽快删除或阻止内容至关重要。互联网的全球性使难上加难：违法者可以在一个国家制作材料，并在另一个国家为第三国的消费者托管。不经过复杂的国际合作，几乎不可能颁布国家授权令或通报。

数字世界中创新的步伐意味着犯罪格局在不断变化。最近出现的主要威胁包括：

¹⁵ 宽带委员会，《儿童在线安全：将在线暴力、虐待和剥削的风险降至最低》（2019年）。

- 加密的兴起无意中允许违法者通过隐藏的渠道操作和共享材料，同时也使检测和执法变得更加困难。
- 致力于诱骗儿童的论坛正在互联网的屏蔽角落中发展，使这种行为常规化并受到鼓励，通常需要加入“新内容”。
- 互联网的快速发展使用户能够在网上踏入尚未制定/实施全面安全策略或相关基础设施的领域。
- 儿童在年幼时使用无人监管的设备，网上的性行为日益常规化。自创的虐待图像数量每年都在上升。

聚焦：自我生成的内容

儿童和青少年可能会拍摄自己的照片或视频。虽然这种行为本身不一定是非法的，而且可能是正常、健康的性发育的一部分，但任何此类内容都有可能在网上或网下传播，伤害儿童或被用作敲诈勒索的依据。尽管一些儿童可能会被迫或被胁迫分享性图像，但其他儿童（尤其是青少年）可能会自愿制作性内容。这并不意味着他们同意或对这些图像的剥削或滥用和/或传播负责。

性传播被定义为“自我制作性图像”¹⁶，或“交换性信息或图像”，以及“通过手机和/或互联网制作、分享和转发性暗示裸体或接近裸体的图像”¹⁷。性短信是一种自我生成的露骨性内容¹⁸，这种行为“在语境、意义和意图方面有着显著的不同”¹⁹。

尽管性行为可能是最常见的涉及儿童的自我生成的露骨性内容，而且通常是由在这一经历中获得快乐的青少年自愿进行的，但也有许多形式的推介性质的性短信。这指的是这项活动的非自愿方面，例如分享或接收推介性的露骨性照片、视频或信息，例如由熟悉或陌生人试图联系、给孩子施加压力或对孩子进行诱骗。性短信也可能是一种性欺凌的形式，在这种情况下，一个孩子被迫把一张照片发给一个男朋友/女朋友/同伴，然后他又在没有得到他们同意的情况下把照片分发给一个同伴网络。

聚焦：网络欺凌

尽管欺凌现象远在互联网出现之前就已存在，但网上欺凌行为的规模、范围和持续性的增加，可能会进一步加剧对受害者来说已经令人颓丧且往往有害的经历。网络欺凌被定义为通过使用计算机、手机和其他电子设备造成的故意和反复伤害。它经常与在学校或其他地方发生的离线欺凌并行发生，它可能具有额外的种族主义、宗教或性别歧视层面，并且可能通过诸如账户黑客、在线传播照片和视频以及全天候有害信息和内容的公布构成离线伤害的延伸。总的来说，网络欺凌是一个社会问题，而不是犯罪性质的问

¹⁶ Karen Cooper等人，《青少年和自拍的性图像：文献综述》，《人类行为中的计算机》第55期（2016年2月）：706–16，<https://doi.org/10.1016/j.chb.2015.10.003>。

¹⁷ Jessica Ringrose等人，《关于儿童、年轻人和‘性短信’的定性研究》— 为全国防止虐待儿童协会（NSPCC）编写的报告”（2012年，英国伦敦：全国防止虐待儿童协会）<http://doi.wiley.com/10.1046/j.1365-2206.1997.00037.x>。

¹⁸ 联合国毒品和犯罪问题办公室（UNODC），《新信息技术对儿童虐待和剥削的影响研究》（2015年，维也纳：联合国），https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf。^[3] UNODC，《新信息技术对儿童虐待和剥削的影响研究》（2015年，维也纳：联合国），第22页。

¹⁹ Cooper和他人，《青少年与自拍性图像》。

题，解决网络欺凌的政策需要一个整体的方法，包括学校、家庭以及至关重要的儿童自身。

聚焦：网上诱骗和性勒索

随着近年来技术的快速进步以及互联网和数字通信接入的增加，针对儿童的在线犯罪行为的风险也不可避免地随之增加。在这些新兴的网上儿童性剥削形式中，有对儿童网上诱骗和性勒索。网上诱骗泛指成人通过使用互联网或其他数字技术与儿童（18岁以下）交朋友和影响儿童的过程，以促进与该儿童的接触或非接触性互动。通过诱骗过程，违法者试图获得孩子的顺从，以保守秘密，避免被发现和惩罚²⁰。重要的是要认识到，同时还存在同伴虐待的情况。

国际刑警组织报告（INTERPOL）说，互联网通过拥有大量容易接近的潜在目标，并使诱骗者能够以吸引儿童的方式展示自己，为诱骗提供了便利。网上儿童性犯罪者使用操纵、胁迫和诱惑减缓抑制，引诱儿童从事性活动。诱骗者通过一个精心设计的程序识别易受伤害的潜在受害者，收集关于儿童家庭支持的情报，并利用压力或羞耻/恐惧对儿童进行性虐待。诱骗者可能会使用成人色情和儿童虐待或剥削材料消除对潜在目标的阻止，使儿童性行为表现为自然和正常的活动。互联网改变了人们互动的方式，并重新定义了“朋友”的概念。诱骗者可以非常容易和迅速地在网上与孩子建立友谊，这迫使人们重新评估传统的“陌生人危险”训诫。

2007年，《欧洲委员会保护儿童免受性剥削和性虐待公约》（《兰萨罗特公约》）首次在一项国际法律文书中正式承认网上诱骗。第23条将“为性目的引诱儿童”定为刑事犯罪，该条要求存在为实施性犯罪而与儿童会面的故意提议，然后是“导致这种会面的实际行为”。在许多诱骗案例中，儿童在网上受到性虐待和性剥削—《兰萨罗特公约》和许多现行国家法律要求的“会面”完全是虚拟的—但是，与实际会面一样，对儿童也同样有害。至关重要的是，对诱骗行为的刑事定罪应延伸至“非亲自会面而是在网上实施的性虐待案件²¹”。

性勒索²²可以作为网上诱骗的一个特征，也可以作为一种独立的违法行为。虽然没有网上诱骗过程也会发生性勒索，但在某些情况下，在线诱骗可能会导致性勒索²³。性勒索可能发生在网上诱骗的情况中，因为诱骗者在行骗过程中通过威胁、恐吓和胁迫操纵和影响孩子发送他们自己的性图像（自我生成的内容）²⁴。如果受害者未能提供所要求

²⁰ 国际失踪和受剥削儿童中心，《为性目的在线诱骗儿童：立法范本和全球审查》，第一版（2017年，国际失踪和受剥削儿童中心），https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf。

²¹ 兰萨罗特委员会，欧洲委员会《保护儿童免受性剥削和性虐待公约》缔约方委员会，《利用信息技术为性目的引诱儿童（诱骗）》，《关于〈兰萨罗特公约〉第23条的意见及其解释性说明》，2015年6月17日，见：<https://edoc.coe.int/en/children-s-rights/7064-lanzarote-committee-opinion-on-article-23-of-the-lanzarote-convention-and-its-explanatory-note.html>（最后访问于2019年11月6日）。

²² 国家失踪和被剥削儿童中心（NCMEC），《性勒索》，见<http://www.missingkids.com/theissues/onlineexploitation/sextortion>（最后访问于2019年11月6日）。

²³ 《保护儿童免受性剥削和性虐待术语指南》，儿童性剥削问题跨机构工作组，2016年1月28日，卢森堡，D.4iii，第27-28页，见：<http://luxembourgguidelines.org/english-version>。

²⁴ 《保护儿童免受性剥削和性虐待术语指南》，儿童性剥削问题跨机构工作组，2016年1月28日，卢森堡，D.4iii，第27-28页，见：<http://luxembourgguidelines.org/english-version>。

的性好处、额外的亲密图像、金钱或其他好处，他或她的图像可能会被公布在网上，目的是造成羞辱或痛苦，或胁迫儿童制作更多的露骨性材料²⁵。

性勒索被称为“虚拟性侵犯”，因为对受害者有类似的情感和心理影响²⁶。在某些情况下，虐待造成的创伤如此之大，以至于受害者试图通过自残或自杀逃避虐待。

欧洲刑警组织（Europol）指出，收集信息以评估影响儿童的性勒索的范围具有挑战性，而且可能严重漏报²⁷。此外，缺乏网上诱骗和性勒索的通用术语和定义是收集准确数据和了解全球问题真实范围的障碍。

2.6 脆弱的儿童

儿童和年轻人可能因为各种不同的原因而变得脆弱。2019年开展的研究指出，“弱势儿童的数字生活很少得到与“现实生活”逆境所得到的同样细致和敏感的关注”。此外，该报告还指出，“他们（儿童和年轻人）充其量只能获得与所有其他儿童和年轻人相同的一般性在线安全建议，但需要专家干预”。

三个具体的脆弱例子包括：移民儿童、自闭症谱系障碍儿童和残疾儿童，但当然还有许多其他群体。

移民儿童

来自移民背景的儿童和年轻人往往带着一套特定的社会文化经历和期望来到一个国家（或已经在那里生活）。虽然技术通常被认为是连接和参与的促进因素，但是在线风险和机会在不同的环境中可能有很大的不同。此外，经验发现和研究显示了数字媒体的一个重要功能：

- （当去一个新的国家旅行时，）适应环境很重要。
- 这是拨款和了解接收国社会/文化的核心职能。
- 社交媒体在保持与家人和同龄人的联系以及获取一般信息方面发挥着关键作用。

除了许多积极的方面，数字媒体也能给移民带来挑战，包括：

- 基础设施 – 考虑网上安全空间非常重要，这样移民儿童和年轻人可以从隐私和安全中受益。
- 资源 – 移民将大部分钱花在预付费电话卡上。
- 融合 – 除了获得技术，移民儿童和年轻人还需要接受良好的数字教育。

²⁵ 《保护儿童免受性剥削和性虐待术语指南》，儿童性剥削问题跨机构工作组，2016年1月28日，卢森堡，D.4iii，第27-28页，见：<http://luxembourgguidelines.org/english-version>。

²⁶ Benjamin Wittes等人，《性勒索：网络安全、青少年和远程性侵》（2016年5月11日，布鲁金斯学会），<https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf>。

²⁷ Europol，《在线性胁迫和勒索作为一种影响儿童的犯罪形式：执法视角》（欧洲网络犯罪中心，2017年5月），https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf。

自闭症谱系障碍儿童（ASD）

自闭症谱系总结了DSM-5行为诊断过程中的两个核心领域：

- 受限和重复的行为（“对一成不变的需要”）；
- 社交和交流行为困难；
- 经常与智力残疾、语言问题和类似问题同时发生。

技术和互联网为儿童和年轻人提供了学习、交流和玩耍的无限机会。然而，除了这些好处之外，患有自闭症的儿童和年轻人可能更容易遭受许多风险：

- 互联网可以给患有自闭症的儿童和年轻人提供他们在线下可能没有的社交机会和特殊兴趣。
- 社会挑战，例如难以理解他人的意图，会让这个群体容易受到怀有恶意的“朋友”的攻击。
- 在线挑战通常与自闭症的核心特征有关：实际、具体的指导可以改善个人的在线体验，但潜在的挑战依然存在。

残疾儿童

残疾儿童在网上面临的风险与非残疾儿童面临的风险有许多相同之处，但他们也可能面临与其残疾相关的特定风险。残疾儿童在其社区参与活动时经常面临排斥、污名化和障碍（身体、经济、社会和态度）。这些经历有助于残疾儿童在网上空间寻求社会互动和友谊。这可以是积极的，可以建立自尊并创建支持网络。然而，这也可能会使他们面临更大的诱骗、网上引诱和/或性骚扰事件的风险。研究表明，在网下经历困难的儿童和受心理社会困难影响的儿童面临更大的风险²⁸。

总的来说，线下受害的儿童很可能在网上成为受害者。这使得残疾儿童在网上面临更高的风险，但他们更需要上网。研究表明，残疾儿童更有可能遭受任何形式的虐待²⁹，特别是更有可能遭受性伤害³⁰。受害可能包括欺凌、骚扰、排斥和基于儿童实际或感知残疾，或基于与其残疾相关的方面，如他们的行为或说话方式、他们使用的设备或服务的歧视。

对残疾儿童进行诱导、网上教唆和/或性骚扰的罪犯不仅包括针对儿童的违法者，还包括针对残疾儿童的违法者。这类违法者可能包括“奉献者” – 对残疾人有性吸引力的非残疾人（最常见的是截肢者和使用助行器的人），其中一些人甚至假装自己是残疾人

²⁸ Andrew Schrock等人，《引诱、骚扰和问题内容》，哈佛大学伯克曼互联网与社会中心，2008年12月，第87期，https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF-LitReviewDraft_0.pdf。

²⁹ UNICEF，《世界儿童现状报告：残疾儿童》，2013年，https://www.unicef.org/publications/files/SOWC2013_Exec_Summary_ENG_Lo_Res_24_Apr_2013.pdf。

³⁰ Katrin Mueller-Johnson, Manuel P. Eisner和Ingrid Obsuth，《身体残疾青年的性受害：患病率、风险和保护因素的审查》，《人际暴力杂志29》第17期（2014年11月）：3180–3206，<https://doi.org/10.1177/0886260514534529>。

³¹。这些人采取的行动可能包括下载残疾儿童的照片和视频（本质上无害），和/或通过专门的论坛或社交媒体账户分享这些照片和视频。

有人担心“分享”（父母在网上分享孩子的信息和照片）会侵犯孩子的隐私，导致欺凌，造成尴尬，或者在以后的生活中产生负面影响³²。残疾儿童的父母可能会为寻求支持或建议分享这些信息，从而使残疾儿童面临更高的不利后果风险。

由于欠缺“无障碍”设计（例如，不允许增加文本大小的应用）、对所请求的便利（例如，屏幕阅读器软件或自适应计算机控制）的拒绝，或者需要适当的支持（例如，指导如何使用设备，一对一支持浏览社交互动³³），一些残疾儿童在使用网络时可能会遇到困难，甚至被排除在在线环境之外。

就合同风险或签署条款和条件而言，残疾儿童接受法律条款的风险更高，有时甚至连成年人都无法理解。

2.7 儿童对在线风险的看法

在世界范围内暴露于暴力，获取不适当的内容、商品和服务；对过度使用的担忧；数据保护和隐私问题是儿童强调的风险³⁴。

青少年报告了一系列关于他们参与数字技术的问题。其中包括广泛讨论的在线安全问题，如害怕与陌生人在线互动、访问不适当的内容或面对恶意软件或病毒，而其他问题涉及他们获取技术的可靠性、父母对他们“私人”网络生活的侵入以及他们的数字读写技能³⁵。

“欧盟儿童在线”研究显示，色情和暴力内容是欧洲儿童最关心的在线问题。总的来说，男孩似乎更受暴力困扰，而女孩则更关心与接触相关的风险³⁶。“高使用率、高风险”国家的儿童对风险的担忧更多。

在拉丁美洲，儿童咨询表明，失去隐私、暴力和骚扰是主要关切³⁷。孩子们报告说被不认识的人联系，尤其是在网上玩游戏的时候。在这种情况下，主要的策略似乎是不与其接触和/或阻止该人。女孩从小就面临社交媒体的骚扰。他们设法独自应对这些形式

³¹ Richard L Bruno, 《奉献者、伪装者和崇拜者：两例人为残疾障碍》, 《性与残疾15》第4期（1997年），18, <https://link.springer.com/content/pdf/10.1023/A:1024769330761.pdf>。

³² UNICEF, 《网络2.0和3.0时代的儿童隐私：政策的挑战和机遇》, Innocenti讨论文件, 2017年3月（UNICEF, Innocenti研究办公室），访问于2020年1月16日。https://www.unicef-irc.org/publications/pdf/Child_privacy_challenges_opportunities.pdf。

³³ 关于这些权利的指南，见《残疾人权利公约》关于无障碍获取的第9条和关于言论和意见自由以及获取信息的第21条。

³⁴ Amanda Third等人, 《数字时代的儿童权利》（墨尔本：青年和良好合作研究中心，2014年9月）http://www.uws.edu.au/_data/assets/pdf_file/0003/753447/Childrens-rights-in-the-digital-age.pdf。

³⁵ Amanda Third等人, 《青年与在线：数字时代儿童对生活的看法》, 《2017年世界儿童状况报告》（悉尼：悉尼西部大学，2017年）。该报告总结了讲24种官方语言的来自26个不同国家的490名10-18岁儿童的观点。

³⁶ Livingstone, S. (2014年), 欧盟儿童在线：发现，方法，建议，伦敦政经学院：欧盟儿童在线, <https://lsdesignunit.com/EUKidsOnline/>。

³⁷ Conectados al Sur network, “Hablatam.”

的暴力，阻止用户，并改变隐私设置。骚扰有时来自不会说西班牙语，但设法给她们发送图片，请求交友并对她们的帖子发表评论的用户。一些男孩也报告说收到了这样的请求。

在世界的许多地方，孩子们对他们在网上面临的一些风险有很好的理解³⁸。研究表明，大多数孩子能够区分网络欺凌和网上玩笑或戏弄，他们认识到网络欺凌有一个公共层面，并且是故意造成伤害³⁹。

³⁸ 自2016年以来，国际电联在COP范畴内就网络欺凌、数字扫盲和儿童在线活动等相关问题与儿童和成人利益攸关方进行了磋商。

³⁹ UNICEF, 《全球儿童在线比较报告》(2019年)。

3 为制定国家保护上网儿童战略做好准备

在制定促进儿童和青年上网安全的国家保护上网儿童战略时，各国政府和政策制定机构需要确定最佳做法，并实现主要利益攸关方的参与。

以下各节重点介绍典型参与方和利益攸关方，并概述他们在保护上网儿童方面的潜在作用和责任。

3.1 参与方和利益攸关方

政策制定机构可确定代表其管辖范围内每一参与方和利益相关方的合适个人、团体和组织。了解他们当前、计划中和潜在的每项活动，对于国家协调和编排保护上网儿童战略十分重要。

儿童和青少年

全世界的儿童和青少年都显示出他们能够轻松地适应和使用各种新技术。在学校中，互联网正变得越来越重要，已成为儿童和青少年开展工作、游戏和交流的一个重要舞台。

根据儿童基金联盟（ChildFund Alliance）最新报告，只有18.1%的受访儿童认为政府在采取行动保护他们。重要的是，政策制定机构需在此方面与儿童接触，同时认识到后者表达意见的权利（《儿童权利公约》（CRC）第12条）。

为了能够保护儿童，政策制定机构应在所有法律文件中对儿童的定义进行标准化。儿童应被定义为18岁以下的任何人。这与《联合国儿童权利公约》（UNCRC）第1条相一致，该条规定：“儿童是指18岁以下的所有人”。公司不应被允许将18岁以下但法定年龄足以同意数据处理的任何人当作成年人对待。这种狭隘的定义没有任何关于儿童发展阶段的证据证明是合理的。这一定义损害了儿童的权利，威胁到他们的安全。

虽然许多儿童似乎对使用技术很有信心，但许多人觉得网上不安全⁴⁰，并对互联网有一些担忧⁴¹。

儿童和青少年缺少对更广大世界的经验，这使得他们在面对一系列风险时易受到伤害。他们有权获得帮助和保护。此外，记住并不是所有的儿童和青少年都将以相同的方式来感受互联网或其它新技术这一点也很重要。一些因身体或其它方面残疾而有特殊需求的儿童，在网络环境中可能会特别容易受到伤害，因此需要额外的支持和帮助。

调查结果再三显示，成人们想象的、儿童和青少年正在网上进行的事情与实际发生的事情可能会大相径庭。半数接受调查的儿童表示，在他们的国家，成年人不听取

⁴⁰ 儿童基金联盟（ChildFund Alliance），“儿童述说对儿童的暴力行为”，拯救为远大梦想发声，2019年，https://childfundalliance.org/zdocs/a9357061-749f-4ebf-a1e9-b1aee81cb216/SVBD-THE_REPORT-digital.pdf。

⁴¹ 欧洲理事会，“这是我们的世界：儿童对如何在数字世界中保护其权利的看法”，儿童协商报告（欧洲理事会儿童权利司，2017年10月），<https://rm.coe.int/it-s-our-world-children-s-views-on-how-to-protect-their-rights-in-the-/1680765dff>。

他们对重要问题的意见⁴²。出于此原因，确保在国家层面做出安排、制定有关该领域的政策、找到适当的机制以便听取所有儿童和青少年的呼声并虑及他们使用这种技术的具体经验，将是十分重要的。

父母、监护人和教育工作者

父母、监护人和教育工作者花在孩子身上的时间最多。他们应接受数字化素养教育，以了解网上环境，从而能够保护儿童，并教会他们如何保护自己。

教育机构特别有责任教育儿童如何在网上保持安全，无论他们是在学校、家里还是在其他任何地方使用互联网；政策制定机构应从人们很小的时候（3至18岁）就将数字化素养纳入国家课程。这将使儿童能够保护自己，了解自己的权利，并因此将互联网当作获取知识的利器⁴³。

应提醒政策制定机构注意到父母和监护人几乎总是他们自己孩子的第一道、最后一道和最佳防线，并为孩子提供支持。然而，当面对互联网时，他们可能会感到有些迷惑。学校再次成为联系父母和监护人的一条重要渠道，使之既意识到新技术具有的各种风险，又意识到新技术具有的众多积极因素。不过，学校不应成为联系父母和监护人的唯一通道。利用众多不同渠道、尽最大可能与尽可能多的父母和监护人实现联系非常重要。业界在支持用户或客户方面发挥着重要作用。父母和监护人可选择管理他们孩子的网上活动和访问，与孩子谈论正确的行为和技术的使用，了解孩子在网上所做的事情，这样家庭对话即可将有关（孩子的）网上和网下体验融为一体。

父母和监护人还需在如何使用电子设备以及如何在互联网上举止得体方面给孩子们做个好榜样。

应提醒政策制定机构，需征询父母和看护人的意见，以获得他们对网上保护其孩子的看法、经验和理解。

最后，政策制定机构可与其他公共机构一起开展提高公众认识的活动，包括针对父母、看护人和教育工作者的活动。公共图书馆、保健站、甚至购物中心和其他主要零售中心都可以提供无障碍的场所来展示电子安全和数字技能信息。在执行这一任务时，政府应确保所提供的建议保持中立，不涉及任何私人利益，并涵盖数字空间内的繁复多样的问题。

业界

业界是生态系统中的关键利益攸关方之一，因为业界拥有政策制定机构需要掌握和理解以便制定法律框架的技术知识。因此，政策制定机构让业界参与制定保护上网儿童法的进程至关重要。

此外，鼓励业界在开发新技术时，将安全设计方式纳入其业务中也很重要。显然，正在开发或提供新技术产品和服务的公司，应帮助其用户了解这些新技术产品和服务是如何工作的，以及如何安全地、恰当地使用这些新技术产品和服务。

⁴² ChildFund Alliance, “儿童述说对儿童的暴力行为”。

⁴³ 联合国儿基会, “儿童与数字连接政策指南”（政策实验室, 数据、研究和政策, 联合国儿童基金会, 2018年6月）, <https://www.unicef.org/esa/media/3141/file/PolicyLab-Guide-DigitalConnectivity-Nov.6.18-lowres.pdf>。

在帮助提高对网络安全问题的认识方面，尤其是在提高儿童和其父母或监护人以及更广大社区对网络安全问题的认识方面，业界也负有重大责任。通过这种参与方式，业界利益相关方将更多地了解其他利益相关方关注的问题以及最终用户面临的风险和危害。有了这些知识，业界可纠正现有的产品和服务，并明确开发工作中存在的危害。

人工智能领域最近取得的进展，为业界建立更健全的制衡机制以识别用户和为儿童提供积极网上行为的有利环境铺平了道路。这些进步也可能给儿童带来新的风险。

在一些国家，互联网通过自我监管或协同监管框架得到管理。然而，一些国家正在考虑或已经实施法律和监管框架，包括公司有义务发现、阻止和/或消除平台或服务对儿童的伤害，并提供明确的报告途径和获得支持的途径。

研究团体和非政府组织（NGO）

在大学和其它研究团体中，很可能有许多学者和专家对互联网的社会和技术问题以及互联网的影响有专业兴趣并具备非常详细的知识。在帮助国家政府和政策制定机构依据确切的事实和良好的证据制定各种战略方面，他们可以成为一种非常有价值的资源。他们还可以作为一种知识界的平衡力量，来平衡有时过于短期和商业化的商业利益。

同样，在非政府组织（NGO）团体中，常常也会有许多专门技术和信息可用作重要的资源，为儿童、青少年、父母、监护人和教育工作者提供服务，帮助推动网络安全议程，更广泛地说，帮助维护公众利益。

执法机构

可悲的事实是，技术虽然奇妙，但它也引起了犯罪和反社会分子的注意。互联网极大地增加了CSAM和其他网络危害的传播。性侵犯者利用互联网对儿童进行最初接触，然后引诱他们进行非常有害的网上或网下接触。欺凌和其它形式的骚扰可对儿童的生活造成巨大伤害，互联网则提供了一种新的侵害形式。

出于这些原因，执法机构全面参与所有总体战略是至关重要的，以便使互联网对儿童和青少年变得更加安全。需要对执法人员进行适当的培训，以便对针对儿童和青少年的互联网相关犯罪行为开展调查。执法人员需要具备适当的技术知识并有权访问取证设施，使他们能够在最短的时间内提取和解释从计算机或互联网上获得的数据。

此外，非常重要的一点是，执法机构应建立明确的机制，使儿童和青少年或者任何公众成员能够举报可能与儿童或青少年网络安全有关的任何事件或问题。例如，许多国家已经设立热线电话，以推动对CSAM的举报，并存在类似的专门机制，以推动对其它种类问题的举报（如欺凌）。政策制定机构应与国际互联网热线协会（INHOPE）合作，支持他们评估和处理关于CSAM的举报，并受益于INHOPE对世界各地组织的援助，在没有热线的地方设立热线。政策制定机构应确保执法部门和其他利益攸关方之间有开放的沟通渠道。执法机构是在各国境内捕获CSAM的主要力量。应建立一套程序来对此类材料进行检查，以便确定是否可以鉴别当地的受害者。当不可能做出鉴别时，应将材料呈送国际刑警组织（INTERPOL），以便纳入ICSE数据库。由于这是一种全球性威胁，因此，政策制定机构需要确保世界各地执法机构之间的国际合作。这将减少正式程序所要求的时间，并方便相关机构做出更快的响应。

社会服务机构

当儿童或青少年已经受到网上伤害或网上虐待时（例如，将其不适当的或非法的照片发布在互联网上），他们可能因此需要专门的和长时间的援助或心理辅导。可能还需要为罪犯提供综合服务和恢复性做法，特别是那些可能曾在网上或网下受到虐待的年轻罪犯。需要对就职于社会服务机构的专业工作人员进行适当的培训，以便他们能够提供此类援助。应通过网上和网下渠道提供支持。

医疗卫生服务机构

暴力侵害儿童案件发生后所需的医疗卫生服务都应纳入国家层面的基本医疗计划之中。医疗卫生机构应强制性报告虐待行为。医疗卫生专业人员应具备适当的装备和知识，以便能够给予儿童这方面的支持。医疗卫生服务应该扩展到包括对儿童心理健康和福祉的支持。

政府部委

保护上网儿童政策将属于若干政府部委的管辖范围，因此，对于任何成功的国家战略和行动计划来说，让所有这些部门参与进来是非常重要的。这些可能包括：

- 内政部
- 卫生部
- 教育部
- 司法部
- 数字/信息部
- 监管机构

监管机构最有能力与政府机构合作，发挥控制者和会计师的作用。这可能包括媒体和数据保护监管机构。

宽带、移动和Wifi网络运营商

运营商可以发现、阻止和报告其网络中的非法内容，并提供家庭友好的工具、服务和配置，供父母在选择如何管理其子女上网时使用。提供商同样要确保公民自由和隐私得到尊重，这一点亦很重要。

儿童权利

独立的儿童人权机构可以在确保保护上网儿童方面发挥重要作用。尽管这些机构的职责各不相同，但通常具有以下职能：

- 监督法律、政策和做法对保护儿童权利的影响；
- 促进国际人权标准在国家层面得到实施；
- 调查侵犯儿童权利的行为；

- 向法院提供关于儿童权利的专业知识；
- 确保听取儿童关于其对人权问题的意见，包括制定相关法律和政策；
- 促进公众对儿童权利的了解和认识；
- 开展人权教育和培训活动。

根据UNCRC第12条，与儿童直接协商是儿童的权利，这一点很重要。独立的儿童人权机构的咨询、调查、提高认识和教育职能都与预防和应对儿童在网上可能遭受的伤害相关。因此，这些机构应成为确立全面的、基于权利的方式的核心，以加强关于保护上网儿童的法律、监管和政策框架，包括与儿童直接协商，这也是UNCRC第12条赋予他们的权利。

最近，也有一些司法管辖区在引入或考虑引入国家机构的例子，这些机构的具体职责是支持网上儿童权利，包括保护他们免受暴力或伤害。如果存在此类机构，则这些机构也应与在国家层面的、加强对上网儿童保护的响应工作密切相关。

3.2 保护上网儿童方面的现有响应机制

面对信息通信技术（ICT）在全世界儿童生活中日益重要的地位以及我们社会中最年轻的人所固有的风险，已经制定了一些倡议，以便在国家和国际层面采取行动。

国家模式

在国家层面，应突出强调几项涵盖保护上网儿童综合框架重要方面内容的立法。这些包括但不限于：

- 视听媒体服务指令（2018年审查，欧盟）
- 《一般数据保护条例》（GDPR）（2018年，欧盟）

成员国在应对网上儿童安全和福祉威胁的监管和制度方面取得了创新发展。对于儿童在网上遇到的CSAM、网络欺凌和其他伤害，没有万全应对方式，但值得注意的是，在过去几年里，已尝试了一些新的方式：

适合年龄的设计守则（2019年，英国）

2019年初，信息专员办公室公布了其“适合年龄的设计守则”提案，以进一步加强对上网儿童的保护。正如UNCRC所规定的那样，拟议的守则以儿童的最大利益为核心，并对业界提出了若干期望，其中包括健全的年龄核实措施，对儿童而言定位服务为默认关闭，业界只收集和保留最低数量的儿童个人数据，产品在设计上是安全的，且说明是适合年龄和易于获取的。

《有害数字通信法》（2017年审查，新西兰）

2015年的立法将网络虐待定为一种特定的犯罪，并重点关注广泛的、从网络欺凌到报复色情的危害。该立法旨在阻止、预防和减少有害数字通信，使发布旨在给他人造成严重精神痛苦的数字通信成为非法行为，并规定了一系列- 10项- 通信原则。立法授予

用户权能，可以在违反这些原则的情况下向独立组织投诉，或在问题未解决时针对信息始作俑者或主人申请法院命令。

电子安全专员（2015年，澳大利亚）

电子安全专员（eSafety Commissioner）是世界上第一个专门致力于网上安全的政府机构。eSafety设立于2015年，其法定职责是就上网安全问题进行领导、协调、教育和提供意见建议，以确保所有澳大利亚人都拥有安全、积极和赋能的上网体验。eSafety负责管理关注一系列危害的调查计划，包括严重的网上儿童欺凌、基于图像的虐待和被禁止的内容。该机构有权进行调查并采取行动来处理涉及此类伤害的投诉或举报 – 在某些情况下，包括有权向个人和网上服务提供商发出移除材料的通知。除了调查权之外，eSafety还采取利用社会、文化和技术举措和干预措施的社区总动员方式。该机构的预防、保护措施和积极努力为上网安全提供了一个全面的方法。

国际模式

在国际和跨国层面，不同利益攸关方发布了相关建议和标准。本指南建立在以下努力的基础之上：

关于执行《儿童权利公约关于买卖儿童、儿童卖淫和儿童色情制品问题的任择议定书》的导则。

欧洲委员会关于在数字环境中尊重、保护和履行儿童权利的导则⁴⁴。

此导则面向欧洲理事会的所有成员国，旨在协助成员国和其他相关利益攸关方采取全面的战略方式，在数字环境中最大限度地实现儿童权利。涵盖的许多主题包括保护个人数据、提供适合儿童不断发展的能力的合适内容、帮助热线和热线、脆弱性和复原力，以及企业的作用和责任。此外，导则呼吁各国让儿童参与，包括参与决策进程，以确保国家政策充分适应数字环境的发展。该导则目前有19种语言版本，并将辅之以一份适合儿童阅读的版本，以及一份政策制定机构手册，后者将提供有关如何执行导则的具体措施。

欧洲理事会 – 兰萨罗特公约

《欧洲理事会保护儿童免受性剥削和性虐待公约》（兰萨罗特公约）要求各国通过“4ps方式” – 预防、保护、起诉和促进国家和国际合作 – 对针对儿童的性暴力行为做出全面回应。《保护儿童免受性剥削和性虐待公约》缔约方委员会（“兰萨罗特委员会”）通过了一些文件，澄清了《公约》在数字环境方面的运作。上述文件包括：关于儿童产生、分享和接收的儿童性暗示或露骨图像和/或视频的意见（2019年6月6日）；关于《兰萨罗特公约》适用于通过使用ICT助长的、针对儿童的性犯罪的解释性意见（2017年5月12日）；根据《兰萨罗特公约》（2016年6月16日）确定的儿童性虐待材料或图像广告或任何其他犯罪的网址声明；以及对《兰萨罗特公约》第23条的意见 – 通过信息通信技术为性目的引诱儿童（诱骗）。兰萨罗特委员会对《公约》的执行情况进行监督：委员会的第2轮专题监督侧重于保护儿童免受ICT促成的性剥削和性虐待：将于2020年公

⁴⁴ 欧洲理事会（2020年），数字环境，<https://www.coe.int/en/web/children/the-digital-environment>。《欧洲理事会在数字环境中尊重、保护和实现儿童权利的导则》是政府间机构通过的第一套此类标准（CM/Rec, 2018年）。

布监督报告。截至2019年，《公约》共有46个缔约国，包括突尼斯 – 第一个加入的非成员国。

欧洲理事会的进一步导则

欧洲理事会的进一步标准和工具有助于集体确定针对所有利益攸关方的综合框架。欧洲理事会的《网络犯罪公约》包含缔约国将一系列与儿童性虐待材料有关的罪行定为刑事犯罪的义务：该公约目前已得到64个缔约国的批准。除其他外，欧洲理事会的重点是增强儿童及其周围的人的权能，使他们能够安全地在数字世界中畅游。这是通过教育手段推动的，包括得到全面修订的《互联网素养手册》（2017年）、《数字化公民教育手册》（2019年）和针对父母的手册（《数字时代的养育 – 保护网上儿童免受性剥削和性虐待的父母指南》（2017年）；数字化公民……和你的孩子 – 每个父母都需要知道和付诸行动的事情（2019年））。最后，欧洲理事会就儿童在数字环境中的权利开展了咨询研究 – 这是我们的世界：儿童对如何在数字环境中保护其权利的看法（2017年），并进行了一些首次重点是关注残疾儿童在数字环境中的经历的咨询研究 – 向前点击两次，向后点击一次：关于数字环境中残疾儿童的报告（2019年）。

上网儿童安全报告

儿童上网安全：最大限度地降低网上暴力、虐待和剥削的风险+上网儿童安全世界宣言⁴⁵。

经合组织（OECD）关于保护上网儿童的建议（2012年/2019-2020年审查）应进一步突出其他国家和跨国倡议，以支持国际合作和国家制定保护上网儿童战略的努力。例如：

国际儿童性剥削图像数据库

由国际刑警组织管理的国际儿童性剥削图像数据库（ICSE数据库）是一个强大的情报和调查工具，方便专业调查人员与世界各地的同事分享数据。ICSE数据库通过国际刑警组织安全全球警察通信系统（称为I-247）提供，使用先进的图像比较软件在受害者、施虐者和地点之间建立联系。ICSE数据库使成员国的认证用户能够实时访问数据库 – 查询现有数据、上传新数据、对材料进行分类和分拣、消除冲突、进行分析并与世界各地的其他专家交流，以回答与儿童性剥削调查有关的问题。

我们保护全球联盟

我们保护（WePROTECT）全球联盟（WPGA）是一项全球性运动，汇集了改变全球处理网上儿童性剥削（OSCE）方式所需的影响力、专业知识和资源。这是政府、全球科技公司和民间团体组织的合作成果，其利益攸关多方的性质在这一领域独一无二。WePROTECT全球联盟的愿景是明确和保护更多的受害者，逮捕更多罪犯，并结束网上儿童性剥削。

WePROTECT全球联盟由若干成分组成，特别是国家响应模式和全球战略响应。更多细节见附录3。

⁴⁵ 宽带可持续发展委员会（2019年），《2019年宽带状况：宽带是可持续发展的基础》，https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf。

2020年儿童上网安全指数

DQ研究所2020年儿童上网安全指数（COSI）是世界上第一个实时分析平台，帮助各国更好地监测其儿童上网安全状况。

COSI以构成COSI框架的六大支柱为基础。支柱一和支柱二 – 网络风险和有节制的数字使用 – 与数字技术的明智使用有关。支柱三和四，即数字能力和指导与教育，与赋能有关。最后两个支柱与基础设施有关，即社会基础设施和连通性支柱。

3.3 应对网上伤害示例

附录4提供若干应对网上伤害的示例。这些示例涵盖教育对策、立法和网上伤害的确定。

3.4 国家保护上网儿童战略的益处

法律的协调一致

所有国家都通过立法来禁止滥用信息通信技术（ICT）达到犯罪或其他目的，这对实现全球网络安全是非常重要的。由于威胁可能来自全球任何一处，因此挑战在范围上固有其国际化特性，需要国际合作、辅助调查以及共同的实体和诉讼法律条款。因此，各国使自己的法律框架协调一致以制止网络犯罪、保护上网儿童和推动国际合作是非常重要的⁴⁶。

制定适当的国家立法、相关的网络犯罪法律框架，并在此方法内，在国际层面协调一致是任何保护上网儿童国家战略取得成功的关键步骤。这首先需要必要的实体刑法条款将这些行为定为犯罪行为，例如计算机诈骗、非法访问、数据干扰、侵犯版权和CSAM，同时也要注意不要过度地将儿童定罪。事实是，这些条款存在于刑法典中，适用于现实生活中的类似犯罪行为，但不意味着也能适用于互联网上的犯罪行为。因此，对当前国家法律做一个全面分析对明确任何可能的差距至关重要。下一步应当是识别和定义法律语言和参考资料，从而帮助国家建立协调一致的网络犯罪法和诉讼规则。各国可使用这些实用工具精心构建网络安全法律框架和相关法律。国际电联与其成员国和该领域的利益攸关方一起合作，并为全球范围内网络犯罪法律的协调一致做了突出贡献。

鉴于技术创新日新月异，已提出自我监管和协同监管，作为过时的现有监管和漫长立法进程的潜在替代解决方案。然而，为了行之有效，监管机构/政策制定机构需要明确确定某些保护上网儿童的目标和挑战，出台清晰明了的审查程序和方法来评估自我监管和协同监管的有效性，且如果自我监管和协同监管未能解决已确定的挑战，则应启动正式的立法程序来解决这些挑战。此外，成功的自我监管措施可在立法过程中逐渐被纳入正式法律，成为法律后盾，以防止某些自我监管举措的实施方面出现倒退或终止。

⁴⁶ 宽带可持续发展委员会（2019年）。

协调

在各方力量和利益攸关方之间很可能已经存在旨在保护上网儿童的一系列活动和行动，但这些活动和行动是孤立发生的。理解这些对于理解在制定国家保护上网儿童战略方面的现有努力很重要。该战略将着眼于通过调整现有和新的活动来协调和指导相关努力。

4 关于框架和实施的建议

各国政府必须解决数字环境中一切形式的暴力侵害儿童行为。然而，为保护数字环境中的儿童而采取的措施不应不适当地限制行使其他权利，如言论自由权、获取信息权或结社自由权。不要因为害怕在网上遇到风险而抑制孩子天生的好奇心和创新意识，关键是要发掘孩子的足智多谋，增强他们的应变能力，同时发掘数字环境的潜力。

许多情况下，对儿童的暴力行为是由其他儿童实施的。在这种情况下，各国政府应尽可能采用恢复性方法来弥补所造成的伤害，同时防止将儿童定罪。各国政府应促进使用ICT来预防和应对暴力，例如开发便于儿童获取信息的技术和资源、屏蔽有害材料并在暴力事件发生时进行报告⁴⁷。

为了应对全球儿童上网安全形势，各国政府必须促进相关实体之间的沟通，并公开合作，消除对上网儿童的伤害。

4.1 有关框架的建议

4.1.1 法律框架

各国政府应审查并在必要时更新其法律框架，以支持在数字环境中充分实现儿童权利。全面的法律框架应涉及预防措施；禁止数字环境中一切形式的暴力侵害儿童行为；提供有效的补救、康复和重返社会手段以解决侵犯儿童权利的问题；建立对儿童敏感的心理辅导、报告和投诉机制；打击有罪不罚现象的问责机制⁴⁸。

立法应尽可能技术中立，以免其适用性受到未来技术发展的影响⁴⁹。

立法的有效实施要求各国政府采取补充措施，包括提高认识和社会动员举措、教育努力和运动以及从事儿童工作的专业人员的能力建设。

在制定适当的法律时，同样重要的是要牢记，儿童不是一个无差异群体。不同年龄阶段的儿童以及有特殊需求或在数字环境中或通过数字环境受到伤害的风险更高的儿童可能需要不同的应对措施。

各国政府应创建明确和可预测的法律和监管环境，支持企业和其他第三方履行其责任，在国内外的业务活动中维护儿童权利⁵⁰。

以下方面将有助于政策制定机构审查任何法律框架的范围和下列规定：

- 性诱骗或其他形式的远程引诱、勒索或胁迫儿童进行不适当的性接触或性活动；

⁴⁷ 负责暴力侵害儿童问题的秘书长特别代表，负责暴力侵害儿童问题的秘书长特别代表提交人权理事会的年度报告，A/HRC/31/20（2016年1月），第103和104段。

⁴⁸ 负责暴力侵害儿童问题的秘书长特别代表，释放儿童的潜力并尽量减少风险：ICT、互联网和暴力侵害儿童，2014年（纽约：联合国），第55页。

⁴⁹ 负责暴力侵害儿童问题的秘书长特别代表，释放儿童的潜力并尽量减少风险：ICT、互联网和暴力侵害儿童，2014年（纽约：联合国），第64页。

⁵⁰ 联合国儿童权利委员会，第16号一般性意见，第53段。

- 确保CSAM的拥有、生产和传播，无论传播意图如何；
- 网上骚扰、欺凌、虐待或仇恨言论；
- 网上恐怖主义材料；
- 网络安全；
- 关于网下非法行为在网上亦同样是非法行为的思考。

4.1.2 政策和制度框架

保证在数字环境中实现儿童权利要求政府在最大限度地增加儿童使用ICT的益处和最大限度地减少相关风险之间取得平衡。这可以通过在国家宽带计划中纳入保护上网儿童的措施⁵¹，以及通过制定一项单独的多层面保护上网儿童战略来实现。这一议程应与任何与儿童权利或儿童保护相关的现有政策框架充分融合，并应进一步补充国家儿童保护政策，为儿童面临的所有风险和潜在伤害提供一个具体框架，以创造安全、包容和赋能的数字环境⁵²。

各国政府应建立国家协调框架，赋予明确的职责和足够的权力，在跨部门、国家、区域和地方各级方面协调与儿童权利和数字媒体及ICT有关的所有活动。各国政府应确立有时间限制的目标和透明的进程来评估和监督进展情况，并必须确保为这一框架的有效运作提供必要的人力、技术和财政资源⁵³。

各国政府应建立利益攸关多方平台，指导国家儿童数字议程的制定、实施和监督。这一平台应汇集最重要的相关方代表，包括儿童和青少年；父母/看护人协会；政府相关单位；教育、司法、卫生和社会保障部门；国家人权机构和相关监管机构；民间团体；业界；学术界；相关专业协会。

4.1.3 监管框架

如果企业未能采取必要、适当和合理的措施来防止和纠正相关侵权，或与之合作或容忍相关侵权，则政府应对商业企业造成或促成的儿童权利的侵权负责⁵⁴。

《工商企业与人权指导原则》预计，公司应提供合法、易于获得、可预测、公平、符合权利、透明、基于对话和参与的补救和申诉机制，以及持续学习渠道。工商企业建立的申诉机制可提供灵活和及时的替代解决方案，有时通过这些机制解决对公司行为提出的关切可能符合儿童的最大利益。在任何情况下，都应能够诉诸法院或对行政补救措施和其他程序进行司法审查⁵⁵。应考虑建立机制，为儿童提供安全、适龄的服务，并方便用户报告他们的关切。

⁵¹ 《2019年宽带状况》，建议5.6，第78页https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf。

⁵² 关于国家宽带计划的儿童保护示范条款，请参见《儿童上网安全报告》第10章。

⁵³ 负责暴力侵害儿童问题的秘书长特别代表，负责暴力侵害儿童问题的秘书长特别代表的年度报告（2014年12月）A/HRC/28/55和释放儿童的潜力并尽量减少风险：ICT、互联网和暴力侵害儿童，2014年（纽约：联合国），第88段。

⁵⁴ 联合国儿童权利委员会，第16号一般性意见，第28段。

⁵⁵ 人权与跨国公司和其他工商企业问题秘书长特别代表的报告，A/HRC/17/31（2011年），第71段。

尽管存在内部申诉机制，但各国政府应建立监督机制，调查和纠正侵犯儿童权利的行为，以期改善ICT和其他相关公司的问责制，并加强监管机构在制定与儿童权利和ICT相关的标准方面的责任⁵⁶。这一点尤其重要，因为那些受到公司行为不利影响的人们可利用的其他补救办法 – 如民事诉讼和其他司法补救 – 往往既麻烦又昂贵⁵⁷。

联合国儿童权利委员会强调了国家人权机构在这一领域的潜在作用，概述了它们如何能够在接受、调查和调解由行业实体造成的侵权投诉方面发挥作用；对大规模侵权行为进行公开调查；进行立法审查，以确保其符合《儿童权利公约》。委员会指出，必要时，“各国应扩大国家人权机构的立法授权，以顾及到儿童权利与工商企业情况”。尤其重要的是，任何投诉机制都应是儿童敏感的，能确保受害者的隐私和保护，并对儿童受害者开展监测、跟进和核实活动。

国家人权机构或其他监管机构可为儿童提供有效补救的一个示例是在出现网络欺凌事件时。在这种情况下，内部补救和申诉机制有时被证明是无效的，因为尽管内容令人苦恼和有害，但国家立法往往没有有关处理这一问题的规定，也没有明确的依据要求内容主人删除相关内容。授权公共当局接受关于网络欺凌案件的投诉，并与内容主人交涉删除相关材料，将是对儿童的一项重要保障⁵⁸，其优势在于提供快速响应 – 这在网络欺凌的背景下至关重要 – 同时也为消除网络欺凌材料提供了明确的法律依据。

在制定数字环境监管方式时，政府还必须认识到这种监管对享有包括言论自由在内的所有人权的影响⁵⁹。

政府应规定企业有义务对儿童权利进行尽职调查。这将确保工商企业能够确定、预防和减轻其对儿童权利的影响，包括其各种业务关系和全球业务的影响⁶⁰。

此外，政府应考虑采取补充措施，如确保其活动可能对数字环境中的儿童权利产生影响的行业实体必须遵守防止和应对潜在侵权行为的最高标准，才有资格获得资金或合同。

4.2 有关实施的建议

各国政府应确保受到权利侵犯的儿童能够获得有效的补救，包括通过适当的赔偿，帮助他们为所遭受的伤害寻求及时和适当的赔偿。各国政府还应为数字媒体和ICT相关侵权行为的儿童受害者提供充分的支持和援助，包括综合服务，以确保儿童完全康复和重返社会，并防止儿童受害者再次受害⁶¹。

应通过法律建立安全和方便获取的儿童敏感心理辅导、报告和投诉机制（如求助热线），并应成为国家儿童保护系统的一部分。重要的是要确保这些服务与任何监管服务相联系，以帮助简化儿童在可能遭遇困境时与机构的互动。求助热线对于诸如性虐待等高度敏感的问题特别有价值，因为儿童可能很难与同龄人、父母、看护人或教师讨论这

⁵⁶ 联合国儿童权利委员会，2014年一般性讨论日报告，第96段。

⁵⁷ 增进和保护见解和言论自由权问题特别报告员报告，A/HRC/32/38（2016年），第71段。

⁵⁸ Bertrand de Crombrughe，“人权理事会第三十一届会议报告”（联合国人权理事会，2016年）。

⁵⁹ 增进和保护见解和言论自由权问题特别报告员报告，A/HRC/32/38（2016年），第45段。

⁶⁰ 联合国儿童权利委员会，第16号一般性意见，第62段。

⁶¹ 联合国儿童权利委员会，2014年一般性讨论日报告，第106段。

些问题。求助热线在引导儿童获得法律服务、安全住所、执法或康复等服务方面也发挥着至关重要的作用⁶²。

此外，政府需要了解和跟踪罪犯的行为，以提高对施虐者的发现率，降低被定罪的施虐者再次犯罪的风险。建立求助热线，为那些对儿童有性兴趣的感觉或想法的人—潜在罪犯—提供免费的匿名电话或基于聊天的心理辅导和支持。帮助罪犯改变他们的行为会将再次犯罪的风险降到最低。

法定投诉处理机制也是有效补救框架的重要组成部分。

监管机构应进行独立衡量和研究，以评估平台如何报告和处理与儿童保护相关的问题。监管机构独立监控平台的技术业已存在。应支持业界提供商发布透明度报告。

各国政府应与国际社会和业界一起，制定一套世界性的衡量标准，方便利益相关方用以衡量儿童上网安全的所有相关方面。

4.2.1 性剥削

政策制定机构在审议对儿童的伤害威胁时的具体考虑，特别是儿童性虐待材料、自创内容、引诱和性虐待以及其他网上风险。这些可包括：

- 中断或减少CSAM通信流量的措施，如，建立国家热线电话或IWF举报门户，以及实施措施阻断对有关网站的访问，因为已知这些网站包含或以广告宣传提供CSAM。
- 确保国家处理程序就位，从而确保在相关国家发现的所有CSAM都传送到集中管理的、拥有指导企业删除内容立法权的国家单位。
- 制定相关战略，以解决对CSAM的需求问题，尤其是那些被判犯有这类罪行的人们的需求。重要的是需意识到这样的事实，即这不是一种无受害者的犯罪行为：为制造可供观看的材料，儿童受到了侵害，且因有意观看或下载CSAM，人们直接对所描绘的儿童侵害形成助纣为虐态势，并怂恿对更多儿童进行侵害，以制作更多的图片。
- 应意识到以下事实，即不论出于制作CSAM的目的，还是以任何其它方式，儿童都绝不会同意遭到性侵害。鼓励使用CSAM的人们寻求帮助，与此同时，让他们意识到他们将为其从事的非法活动承担刑事责任。
- 解决对CSAM的需求问题的其他战略。例如，一些国家保留被定罪的性犯罪者的登记册。法院已颁布司法命令，完全禁止这些性侵犯者使用互联网，或者禁止这些性侵犯者使用儿童和青少年经常光顾的那部分互联网。迄今为止，这些命令的问题在于执行。不过，一些国家正考虑将已知的性侵犯者名单结合进网站禁访清单（block list）中，从而防止名单上的人员访问或连接某些网站，例如，已知有大量儿童和青少年访问的网站。当然，如果性侵犯者使用不同的名字或伪造的登录名接入某个网站，那么此类措施的有效性将大大降低，但通过判定这种行为有罪，可起到进一步的威慑作用。
- 为受害者提供适当的长期援助。当儿童或青少年已遭受网络欺凌时，例如，当他们的非法图像已出现在了互联网上时，自然地，他们会非常关心谁可能会看到这些图

⁶² 负责暴力侵害儿童问题的秘书长特别代表，释放儿童的潜力并尽量减少风险，第51页和第65页。

像以及这将对他们产生什么影响。这将使儿童或青少年感到受到更容易被欺凌或受到更多的性虐待和性侵害。在这方面，重要的是提供专业支助服务，以支助处于这种情况下的儿童和青少年。此类支助可能需要长期提供。

- 确保建立一种机制，并推广应用，以便提供一种易于理解的和快速的手段，举报非法内容或非法的或令人不快的网上行为，例如，一种类似于“[虚拟全球任务组和INHOPE](#)”所建的系统。应鼓励使用INTERPOL i24/7系统。
- 确保在调查互联网和计算机犯罪过程中，有足够数量的执法人员接受过适当的培训，并有权访问适当的取证设施，使之能够提取和解释相关的数字数据。
- 投资培训执法、检察和司法部门人员，让他们了解网络犯罪分子实施这些犯罪的方法。也需要投资采办和维护好相关设施，以便从数字设备中获取和解释各种取证证据。此外，与其它国家的相应执法部门和调查机构开展双边和多边协作和信息交换也是非常重要的。

4.2.2 教育

对儿童进行数字化素养教育是确保他们可以从技术中受益且免受伤害的战略的一部分。这将促进儿童发展批判性思维技能，帮助他们明确和理解他们在数字空间中行为的好和坏的方面。虽然向儿童图文并茂地说明网上可能发生的伤害很重要，但只有作为更广泛的数字化素养方案——该方案应适合儿童的年龄并侧重于技能和能力——的一部分，这种说明才会有效。将社会和情感学习概念纳入上网安全教育非常重要，因为这些概念将有助于学生理解和管理情感，从而在网上和网下都可建立健康和相互尊重的关系。

儿童应有适当的工具和知识来应对互联网是保持他们安全的最佳方法之一。在学校课程中引入数字化素养内容是一种方式。另一种可能性是在学校课程之外创建教育资源。

从事儿童工作的人员应具备适当的知识和技能，能够自信地支持儿童应对和解决与保护上网儿童相关的问题，并向儿童提供必要的数字技能，以便成功地从技术中受益。

4.2.3 业界

国内和国际业界参与方应努力提高对儿童上网安全问题的认识，并帮助所有负责儿童福祉的成年人（包括父母和看护人、学校、青年服务组织和社区）开发保护儿童安全所需的知识和技能。业界应对其产品、服务和平台采用更安全的设计方式，将安全视为核心目标。

- 提供适合年龄的家庭友好工具，帮助用户更好地管理对其家庭的上网保护。
- 为用户提供适当的举报机制，以报告问题和顾虑。用户应期望这些报告能及时得到响应，了解到有关所采取措施的信息，如果适用，还应提供用户可获得进一步支持的地方。
- 此外，提供针对虐待儿童的主动举报机制，以发现和解决针对儿童的任何类型的虐待（归类为犯罪活动）。这一做法表明，如果所有利益攸关方都参与发现、阻止和

报告行动，则我们就能为所有人创造更清明、更安全的互联网环境。业界应考虑使用所有相关工具，例如IWF服务，来防止其平台被人利用。

让生态系统中的所有相关参与方都参与进来至关重要，他们应意识到网上风险和危害，以便能够防止儿童面临不必要的风险。

制定儿童上网安全的共同指标，以衡量问题的所有相关方面。只有通过共同的标准和衡量指标，才能跟踪各国的进展情况，确定为消除任何针对儿童的暴力行为和承认儿童上网安全生态系统的力量而实施的项目和活动是否成功。

5 制定国家保护上网儿童战略

5.1 国家战略要素清单

为了阐明国家针对网上儿童安全的重点战略，政策制定机构需要考虑一系列战略。表1列出需要考虑的关键领域。

表1：需要考虑的关键领域

	#	需要考虑的关键领域	更多细节
法律框架	1	审议现有的法律框架，以确定存在一切必要的法定权力使执法机构和其他相关机构能够保护18岁以下的人在所有互联网平台上的网上安全。	一般来说，有必要制定一套法律，明确规定在现实世界中儿童犯下的任何和每一项罪行，经适当变通后，也可能在互联网或任何其他电子网络上犯下。
	2	建立原则上适用的法律规定，在现实世界中任何对儿童违法的行为在网络世界也属非法，对法律上的未成年人的网上数据保护和隐私条例也要充分适当。	也可能有必要制定新的法律或调整现有法律，规定某些只可能发生在互联网上的行为不合法，例如在线引诱儿童进行或观看色情表演，或“诱骗”儿童出于性目的在现实世界中见面。 除这些目的外，通常还需要有一个法律框架，规定禁止为犯罪目的滥用计算机，禁止入侵（黑客）或其他恶意或未经同意的对计算机代码的使用，并警示人们互联网可成为犯罪场所。

	#	需要考虑的关键领域	更多细节
监管框架	3	<p>考虑监管政策的制定，其中可能包括自我或协同监管政策以及全面监管框架的制定。</p> <p>自我监管或协同监管模式可包括制定和发布良好做法守则或网上基本安全期望，既有助于所有相关利益攸关方的参与、协调或配合和持续参与，也有助于加快制定和实施适当技术变革应对措施的速度。</p> <p>监管模式可确定所有利益相关方的期望和义务，并将其纳入法律范畴。也可考虑对违反政策行为实施处罚。</p>	<p>有些国家已在该领域建立与政策制定相关的自我监管或协同监管的模式。例如，通过这类模式，国家可以颁布良好行为守则，以指导互联网界采取最有效措施，使网上儿童和青少年更加安全。例如在欧盟国家，向那些通过网络为儿童和青少年提供内容和服务的社交网站和移动电话网，公布了欧盟范围内的使用守则。在提高对技术变化做出适当反应的速度方面，自我监管或协同监管可以更加灵活。</p> <p>最近，一些国家制定和/或实施了监管框架。在这些示例中，监管框架是从自我或协同监管模式中产生的，确定了利益攸关方（尤其是业界提供商）更好地保护其用户的要求和期望。</p>

	#	需要考虑的关键领域	更多细节
举报 – 非法内容	4	<p>确保建立机制并广泛推广以提供一种易于理解的方式来举报互联网上出现的非法内容，例如，国内热线电话能够快速响应并把非法内容删除或使其无法访问。</p> <p>业界应利用与其组织相关的所有服务，通过建立机制来识别、屏蔽和消除网上虐待儿童的内容。</p>	<p>应在国际互联网和其它媒体上，广泛宣传并推动网上服务滥用举报机制或者令人讨厌的或非法的网上行为举报机制，例如，举报给国家某条热线电话。如果没有国家热线，则IWF提供举报门户解决方案。</p> <p>应在允许显示用户自创内容的任何网站的相应位置上，突出显示至虐待举报机制的链接。也应使以某种方式感到受互联网威胁的人们或者目击互联网上令人担忧行为的人们，能够尽快将之举报给相应的执法机构。需要对这些执法机构进行培训，以便随时做出响应。“虚拟全球任务组”就是这样一个执法机构，它提供一种每周7天、每天24小时（24/7）的响应机制，以接收来自美国、加拿大、澳大利亚和意大利的、有关非法网络行为或非法网络内容的举报，还有其它一些国家也想尽快加入该机制。有关信息请参见：www.virtualglobaltaskforce.com。另见INHOPE。</p>
报告 – 用户的关切	5	<p>业界应为用户提供报告关切和问题的机会，并做出相应的回应。</p>	<p>提供商必须有义务为他们的用户提供明确的路标，让他们能够报告服务中的问题和顾虑。其形式应是儿童喜闻乐见的和容易获得的。</p>

	#	需要考虑的关键领域	更多细节
参与方和利益攸关方	6	<p>让所有对保护上网儿童感兴趣的相关利益相关方参与进来，特别是：</p> <ul style="list-style-type: none"> • 政府单位 • 执法机构 • 社会服务机构 • 互联网服务提供商（ISP）和其他电子服务提供商（ESP） • 移动电话网提供商 • 公共Wi-Fi网提供商 • 其他相关高科技公司 • 教师组织 • 家长组织 • 儿童和青少年 • 保护儿童组织和其他相关非政府组织 • 大专院校和研究机构 • 网吧业主和其他提供公共上网的场所，例如图书馆、电信中心、PC Bangs⁶³和网络游戏中心等。 	<p>一些国家政府发现，将所有主要利益攸关方和参与者聚集一起，集中精力制定和实施一项国家举措，使互联网成为儿童和青年人更安全的地方，并提高对这些问题以及如何以非常实际的方式处理这些问题的认识，是非常有益的。</p> <p>在该战略中，重要的是要意识到现在许多人可通过多种不同设备普遍和永久与互联网连接。宽带、移动和Wi-Fi运营商都应参与其中。另外，在许多国家，公共图书馆、电信中心和网吧也是上网的重要场所，对儿童和青少年来说尤其如此。</p>
研究	7	对国家各种参与方和利益攸关方进行研究，以确定他们在保护上网儿童方面的意见、经验、关切和机会。这也应认识到保护上网儿童的责任范围以及现有或计划的相关活动。	

⁶³ “PC Bang”一词通常用于韩国和一些其他国家，表示一个大游戏厅，通过局域网使玩家可以通过网络玩大型游戏，或者在游戏厅内的玩家之间玩游戏。

	#	需要考虑的关键领域	更多细节
数字化素养和能力教育	8	<p>培养数字化素养是任何适龄并适用于所有儿童的国家学校课程的一部分。</p>	<p>学校和教育系统通常是国家保护上网儿童战略的教育和数字化素养组成部分的基础。</p> <p>国家的任何学校课程都应包括保护上网儿童的内容，并旨在为所有年龄的儿童提供适当的技能，使其受益于并成功使用技术，并对要成功避免的威胁和伤害保持敏感。这类内容应认可和奖励积极和具有建设性的网上行为。</p> <p>在任何教育和提高认识活动中，找到正确基调十分重要。应避免带来恐慌的信息，且应重点强调新技术的许多积极有趣的特点。互联网有巨大的潜力促使儿童和青少年更主动地去发现新世界。教会他们积极和负责的网上行为方式是教育和提高认识方案的关键目标。</p> <p>从事儿童工作的人员，特别是教师，应得到适当的培训和手段，以便成功地教育儿童并向儿童提供这些技能。他们应了解网上的威胁和伤害，并有能力自信地洞悉虐待和伤害的蛛丝马迹，以便为保护他们的孩子而对这些问题做出响应和举报。</p>

	#	需要考虑的关键领域	更多细节
教育资源	9	<p>利用所有利益攸关方的知识和经验，开发反映本地文化规范和法律的互联网安全信息和资料，并确保这些资料有效地得到传播并恰当地呈现给所有关键目标用户。在宣传提高认识信息时要考虑谋求大众媒体的帮助。制定资料时要侧重于互联网对儿童和青少年积极和赋予能力的方面，避免带来恐慌的信息。提倡积极和负责任的网上行为方式。</p> <p>考虑开发资源，帮助父母评估自己孩子的网上安全情况，并学习如何通过有针对性的教育，最大限度地降低风险，最大限度地发挥自己家庭的潜力。</p>	<p>当制作教育材料时，重要的是要考虑到许多不懂技术的人使用起来会觉得不舒服。为此，确保以纸质形式提供安全材料或用不懂技术的人员更为熟悉的其他媒介，例如视频，来制作安全材料，这一点也很重要。</p> <p>许多大的互联网公司创建网站，包含大量有关儿童和青少年上网问题的信息。然而，这些材料常常只以英文或以非常小范围的语言提供。因此，制作能反映本国法律和本地文化规范的本地化材料非常重要。这对开展互联网安全活动或开发培训材料都是非常必要的。</p>
保护儿童	10	<p>确保普遍和系统性的儿童保护机制已经到位，规定所有从事儿童工作的人员都有义务发现、应对和报告网上发生的虐待和伤害事件。</p>	<p>应出台适用于所有从事儿童工作人员的普遍性儿童保护制度，要求这些人员报告虐待或伤害儿童事件，以便调查和解决问题。</p>
国家范围的提高认识活动	11	<p>组织全国性的提高认识活动，创造机会广泛强调保护上网儿童问题。利用“更安全的互联网日”等全球性活动来开展活动可能会有所裨益。</p>	<p>父母和监护人以及专业人士，例如老师，在协助保护上网儿童和青少年安全中起着至关重要的作用。应制定支助方案，帮助提高对这些问题的认识，并提供处理这些问题的战略。</p> <p>也应考虑谋求大众媒体的帮助，以宣传提高认识的信息和活动。</p> <p>“更安全的互联网日”等机会将有助于促进和鼓励关于保护上网儿童的全国性对话。许多国家成功地围绕“更安全的互联网日”开展了全国性的提高认识活动，并让所有参与方和利益攸关方在媒体和社交媒体上参与最广泛的信息传播活动。</p>

	#	需要考虑的关键领域	更多细节
工具、服务和设置	12	<p>考虑设备设置、技术工具（如过滤程序）以及可助一臂之力的儿童保护应用和设置的作用。</p> <p>通过鼓励更新操作系统以及使用合适的安全软件和应用程序，鼓励用户对他们的设备负责。</p>	<p>目前有若干服务可用以帮助屏蔽有害材料或阻断有害连接。其中一些此类儿童安全和过滤程序基本上是免费的，原因是它们是计算机操作系统的一部分，或是ISP或ESP提供之软件包的一部分。如果设备具有互联网功能，则一些游戏机制造商也提供类似的工具。这些程序并非万无一失，但可以提供良好的支持，尤其是对有年幼子女的家庭。</p> <p>大多数设备都配有有助于保护儿童和促进健康平衡使用的设置。可将此延伸至相关机制，以便于父母管理其孩子的设备、分配时间、管理孩子能够使用的应用和服务并管理孩子的购买行为。</p> <p>最近开发了报告和设置，使用户和父母能够更好地了解和管理屏幕时间和访问情况。</p> <p>这些技术工具应作为更大工具库的一部分来使用。父母和/或监护人的参与至关重要。随着儿童开始长大，他们想拥有更多的隐私，并更强烈地想探索自身的价值。此外，在供应商和客户之间存在计费关系的情况下，年龄核实流程可发挥非常有价值的作用，帮助年龄受限的商品和服务供应商或仅面向特定年龄或特定年龄以上受众的材料出版商接触这些特定受众。如果不存在计费关系，则年龄核实技术的使用可能会有问题，或在许多国家，由于缺乏可靠的数据来源，几乎不可能使用年龄核实技术。</p>

5.2 问题示例

随着国家利益攸关方和参与方的确定，可将以下问题分发给利益攸关方和参与方，并请他们填写答案。他们的答案将有助于确定政策覆盖范围、优势以及国家战略要素清单中的重点领域。

- 贵方在网上安全和儿童权利方面负有何种程度的责任？
- 网上安全和儿童权利是如何融入贵方现有的政策和程序中的？
- 现有法律在多大程度上涵盖了网上安全？
- 贵方的网上安全重点是什么？
- 贵方有哪些支持网上安全的活动？
- 贵方如何与其他机构和组织合作来改善/提高网上安全？
- 儿童/父母可向贵方报告网上安全问题吗？
- 贵方在网络世界中面临的三大挑战是什么？
- 贵方在网络世界中面临的三大机遇是什么？

开展研究并了解儿童及其父母对保护上网儿童的看法和经验也将有所帮助。

6 参考资料

网上儿童安全：主要文件和出版物

2020年

- ECPAT国际，[中东和北非儿童的性剥削](#)，2020年
- DQ研究所，[2020年网上儿童安全报告](#)，2020年
- 欧盟上网儿童，[2020年欧盟上网儿童调查：来自19个国家的调查结果](#)，2020年

2019年

- 互联网观察基金会（IWF），[年度报告](#)，2019年
- WeProtect全球联盟，[全球威胁评估](#)，2019年
- 国际电联/联合国教科文组织宽带委员会，[网上儿童安全世界宣言](#)，2019年。
- 国际电联/联合国教科文组织宽带委员会，[网上儿童安全：将网上暴力、虐待和剥削风险降至最低](#)，2019年
- [全球上网儿童，在互连世界中成长](#)，2019年
- [重新思考互联网上儿童性虐待图像的发现](#)，2019年5月13日至17日在美国旧金山举行的2019年万维网大会记录，2019年
- [网上危害白皮书（仅限英国）](#)，2019年
- PA咨询，[错综复杂的网络：重新思考网上CSEA方式](#)，2019年
- 英国信息专员办公室，[关于帮助保护上网儿童的行为守则的磋商（仅限英国）](#)，2019年
- 全球终止暴力侵害儿童基金，[终止伤害：了解网上儿童性剥削和虐待的证据](#)，2019年
- [终止暴力侵害儿童全球伙伴关系，安全学习行动呼吁，青年宣言](#)，2019年
- 联合国教科文组织，[数字背后：结束校园暴力和欺凌](#)，2019年（包括网上伤害行为和网络欺凌数据）
- 联合国人权事务高级专员办事处，[与数字环境相关的儿童权利](#)，2019年
- 澳大利亚eSafety专员，[设计安全概述](#)，2019年
- 联合国儿童基金会，[为何企业应投资于数字儿童安全](#)，2019年
- 美国国务院，[人口贩卖报告](#)，2019年

2018年

- WeProtect全球联盟，全球威胁评估，2018年
- 数字世界中的儿童尊严，技术工作组报告，2018年欧洲理事会，部长委员会向成员国提出的关于在数字环境中尊重、保护和实现儿童权利的导则的建议CM/Rec (2018) 7，2018年
- 终止暴力侵害儿童行为全球基金，两年支助解决方案：基金投资结果，2018年
- WeProtect全球联盟，国家应对能力和实施模式的活生生示例，2018年
- 国际刑警组织和ECPAT国际，制定关于儿童性剥削材料中身份不明受害者的全球指标，2018年
- 欧洲刑警组织，互联网有组织犯罪威胁评估（IOCTA），2018年
- NetClean，关于儿童性虐待网络犯罪的报告，2018年
- 失踪和受剥削儿童国际中心（ICMEC），儿童性虐待材料：示范立法和全球审查，第9版，2018年
- 失踪和受剥削儿童国际中心（ICMEC），儿童保护研究：性勒索和非自愿色情制品，2018年
- 国际互联网热线协会，INHOPE报告，2018年
- 互联网观察基金会（IWF），年度报告，2018年
- Thorn，制作和活跃交易描绘已确认受害者的儿童性剥削图像，2018年
- 国际电联，全球网络安全指数，2018年
- CSA专业知识中心，对网上儿童性剥削犯罪者的干预 – 范围审查和差距分析，2018年
- NatCen，网上协助CSEA犯罪人的行为和特征 – 快速证据评估，2018年
- 儿基会，儿童与数字连接政策指南，2018年

2017

- 国家失踪和受剥削儿童中心（NCMEC），网上诱惑儿童：关于CyberTipline报告的深入分析，2017年
- 5权利（5 Rights）基金会，数字童年，解决数字环境中的儿童发展阶段问题，2017年
- Childnet，DeShame报告，2017年
- 加拿大儿童保护中心，幸存者调查，2017年
- 互联网观察基金会（IWF），年度报告，2017年

- 失踪和受剥削儿童国际中心（ICMEC），[年度报告](#)，2017年
- 失踪和受剥削儿童国际中心（ICMEC），[为性目的在网上诱骗儿童：示范立法和全球审查](#)，2017年
- Thorn，[对2097名年龄在13岁到25岁之间的性勒索受害者进行的网上调查](#)，2017年
- 儿基会，[数字世界中的儿童](#)，2017年
- 西悉尼大学，[年轻与上网：数字时代儿童对生活的看法](#)，2017年
- ECPAT国际，[东南亚的儿童性剥削](#)，2017年

2016

- 联合国儿童基金会，[危险与可能性：网上成长](#)，2016年
- 儿基会，[数字时代的儿童保护：东盟国家对网上CSEA的回应](#)，2016年
- 司法和犯罪预防中心，[中东和北非地区的网上儿童保护](#)，2016年
- ECPAT国际，[儿童性剥削问题机构间工作组，保护儿童免受性剥削和性虐待术语导则（卢森堡导则）](#)，2016年

2015

- WeProtect全球联盟，[预防和解决儿童性剥削和性虐待问题（CSEA）：国家应对模式](#)，2015年
- NCMEC，[全球对抗CSAM热线纵览](#)，2015
- 国际电联和儿基会，[保护上网儿童行业导则](#)，2015年

与数字世界中的人权相关的出版物

- 欧洲理事会，[在数字环境中尊重、保护和实现儿童权利的导则](#)，2018年
- 教科文组织，[互联网普及性指标](#)，2019年
- 数字版权排名（RDR），[2019年RDR企业责任指数](#)，2019年
- 宽带可持续发展委员会，[宽带状况](#)，2019年
- 国际电联，[衡量数字发展](#)，2019年
- 国际电联，[衡量信息社会报告](#)，2018年
- 儿基会，[儿童与数字营销行业工具包](#)，2018年
- 宽带可持续发展委员会，[数字卫生](#)，2017年
- 宽带可持续发展委员会，[生活和工作的数字技能](#)，2017年
- 宽带可持续发展委员会，[数字性别鸿沟](#)，2017年

- 儿基会，隐私、个人信息和声誉保护，2017年
- 儿基会，言论、结社、获取信息和参与自由，2017年
- 儿基会，互联网接入与数字化素养，2017年
- 联合国儿童权利委员会，关于执行《儿童权利公约关于买卖儿童、儿童卖淫和儿童色情制品问题的任择议定书》的导则，2019年

有关更多资源，请参考www.itu-cop-guidelines.com 上列出的更多资料。

附录1：术语

以下定义主要取自1989年《儿童权利公约》、儿童性剥削问题机构间工作组编制的2016年《保护儿童免受性剥削与性虐待术语导则》⁶⁴（卢森堡导则）、欧洲理事会2012年《保护儿童免受性剥削与性虐待公约》⁶⁵以及2019年《全球上网儿童报告》⁶⁶中的现有术语。

青少年

青少年指年龄在10-19岁的人。请特别注意：在国际法中，“青少年”一词并不具有约束力。年龄在18岁以下的均视为儿童，而19岁则视为成人，除非国家法律规定成年的法定年龄低于18岁⁶⁷。

人工智能（AI）

从最广义上讲，该术语既指纯粹科幻小说中的系统（所谓的“强”人工智能，具有自我意识构成），亦指已投入运行且能够执行高难度任务的系统（面部或语音识别、车辆驾驶—这些系统称为“弱”或“中度”人工智能）⁶⁸。

人工智能系统（AI）

人工智能系统是一个基于机器的系统，能够对一组人类定义的目标，做出预测、建议或影响真实或虚拟环境的决定，可在不同自主程度下运行⁶⁹。

儿童的最大利益

形容在具体情况下针对特定的一名儿童或一群儿童做出决定时所需考虑的所有要素⁷⁰。

儿童

根据《儿童权利公约》第1条，儿童系指18岁以下的任何人，除非国家法律规定的成年年龄低于18岁⁷¹。

⁶⁴ 《保护儿童免受性剥削与性虐待卢森堡术语导则》2016年，114，<http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-EN.pdf>。

⁶⁵ 欧洲理事会《保护儿童免受性剥削与性虐待：欧洲理事会公约》（斯特拉斯堡：欧洲理事会2012年出版），https://www.coe.int/t/dg3/children/1in5/Source/Lanzarote%20Convention_EN.pdf。

⁶⁶ Globalkidsonline.net（2019年），“如果使用得当，互联网可改善学养、提高技能”，2019年11月，<http://globalkidsonline.net/synthesis-report-2019/>。

⁶⁷ 儿基会和国际电联《保护上网儿童行业导则》，（itu.int/cop，2015），https://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf。

⁶⁸ 欧洲理事会，“什么是人工智能？”，coe.int，人工智能，2020年1月16日获取，<https://www.coe.int/en/web/artificial-intelligence/what-is-ai>。

⁶⁹ 经合组织，理事会关于人工智能的建议（2019年，OECD），<https://webcache.googleusercontent.com/search?q=cache:hTtMv9k1ak8J:https://legalinstruments.oecd.org/api/print%3Fids%3D648%26lang%3Den+&cd=3&hl=en&ct=clnk&gl=ch&client=safari>。

⁷⁰ 人权高专办（OHCHR），《儿童权利公约》，2020年1月16日获取，<https://www.ohchr.org/en/professionalinterest/pages/crc.aspx>。

⁷¹ OHCHR、儿基会和国际电联，《保护上网儿童业界导则》。

儿童性剥削和性虐待（CSEA）

指一切形式的性剥削和性虐待（1989年《儿童权利公约》第34条），如“（a）引诱或强迫儿童从事任何非法的性活动；（b）利用儿童卖淫或从事其他非法的性行为；（c）利用儿童进行淫秽表演和充当淫秽题材”以及“未经同意的性接触，通常涉及暴力”。通过互联网或与网上环境的某些连接对儿童实施的性剥削和性虐待日益增加⁷²。

儿童性（剥削和）虐待材料（CSAM）

ICT的迅速发展产生了新形式的网上儿童性剥削和性虐待，可通过虚拟形式实施，且不一定含有与儿童的现场面对面见面⁷³。尽管许多司法管辖区仍将儿童性虐待图像和视频称为“儿童色情制品”或“儿童猥亵图片”，但本指南将此类主题统称为儿童性虐待材料（以下称为CSAM）。这符合宽带委员会导则和WePROTECT全球联盟国家响应模式⁷⁴。这一术语更准确地描述内容。色情制品系合法的商业化行业，卢森堡导则阐述了该术语的用法：

“可能（无意或有意）将实质为对儿童性虐待和/或性剥削行为的严重性降低、淡化甚至合法化[……]‘儿童色情制品’一词可能暗示行为经儿童同意开展，是合法的性材料”⁷⁵。

CSAM一词指表现对儿童进行性虐待和/或剥削行为的材料。其中包括但不限于记录成年人对儿童性虐待的材料；包含在直接性行为中的儿童图像；主要用于性目的制作或使用的儿童性器官图像。

儿童和青少年

系指18岁以下的所有人，其中儿童（在本指南中也称为低龄儿童）涵盖15岁以下的所有人，而青少年则由15至18岁年龄组人群构成。

联网玩具

联网玩具使用Wi-Fi和蓝牙等技术与互联网连接，一般与配套应用结合使用，以实现儿童的交互式玩耍。据Juniper研究机构称，2015年联网玩具的市场达到28亿美元，预计到2020年将增至110亿美元。这些玩具收集并存储儿童的个人信息，包括姓名、地理定位、地址、照片、音频和视频记录⁷⁶。

网络欺凌（亦称网上欺凌）

⁷² “保护儿童免受性剥削与性虐待卢森堡术语导则。”

⁷³ “保护儿童免受性剥削与性虐待卢森堡术语导则”；儿基会“《全球上网儿童比较报告》”，（2019年）。

⁷⁴ WePROTECT全球联盟，防止和处理儿童性剥削和性虐待问题（CSEA）：国家响应模式，（2016年），<https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1479255310190/WePROTECT+Global+Alliance+Model+National+Response+Guidance.pdf>；宽带委员会，“儿童上网安全：尽全力降低网上暴力、虐待和剥削风险（2019年）。”

⁷⁵ “保护儿童免受性剥削与性虐待卢森堡术语导则。”

⁷⁶ Jeremy Greenberg，“危险游戏：联网玩具、COPPA和安全隐患”，乔治城法律技术评论，2017年12月4日，<https://georgetownlawtechreview.org/dangerous-games-connected-toys-coppa-and-bad-security/GLTR-12-2017/>。

国际法没有定义网络欺凌。在本文件中，网络欺凌指团体或个人使用数字技术，针对无法轻易自卫的受害者反复实施的蓄意攻击行为⁷⁷。这种行为通常涉及“使用数字技术和互联网发布关于某人的伤害性信息，以伤害性方式故意共享私人信息、照片或视频，发送威胁性或侮辱性消息（通过电子邮件、即时消息、聊天、短信），散布有关受害者的谣言和虚假信息，或故意将其排除在网上通信之外”⁷⁸。此类行为可能涉及直接通信（如聊天或文本消息）、半公开通信（如在电子邮件通讯录里发送骚扰信息）、或公开通信（如创建专门取笑受害者的网站）。

网络仇恨、歧视和暴力极端主义

“网络仇恨、歧视和暴力极端主义是网络暴力的一种特殊形式，针对集体身份，而非个人[……]通常涉及种族、性取向、宗教、国籍或移民身份、性别和政治”⁷⁹。

数字化公民

数字化公民指基于有效通信和创造的技能，积极、批判性且出色地参与数字化环境的能力，通过负责任地使用技术，实践尊重人权和尊严的社会参与形式⁸⁰。

数字化素养

数字化素养指在日益通过互联网平台、社交媒体和移动设备等数字技术进行通信和获取信息的社会，拥有生活、学习和工作所需的技能。⁸¹其中包括清楚的沟通、技术技能和批判性思维。

数字化复原力

该术语形容儿童在情绪方面处理网上遇到的伤害的能力。数字化复原力包括当孩子面临网上风险时，拥有理解所需的情绪资源，在问题出现时知道如何寻求帮助，吸取经验并恢复⁸²。

教育工作者

教育工作者是通过系统化工作提高他人对特定问题的理解的人。教育工作者的角色包括课堂教学的和相对非正式的教育工作者，例如使用社交网站平台和服务提供上网安全信息或运营社区或基于学校的课程，使儿童和青少年能够确保上网安全的人。

⁷⁷ Anna Costanza Baldry、Anna Sorrentino和David P. Farrington（2019年），“网络欺凌和网络受害与父母对青少年上网活动的监督、监控和控制”96（2019年1月）：302–7，<https://doi.org/10.1016/j.childyouth.2018.11.0058>。

⁷⁸ 儿基会“《全球上网儿童比较报告》”，（2019年）“保护儿童免受性剥削与性虐待卢森堡术语导则”。

⁷⁹ 儿基会“《全球上网儿童比较报告》”，（2019年）。

⁸⁰ 欧洲理事会，“数字化公民与数字化公民教育”，数字化公民教育，2020年1月16日获取，<https://www.coe.int/en/web/digital-citizenship-education/home>。

⁸¹ 西悉尼大学Claire Urbach，“什么是数字化素养？”，2020年1月16日获取，https://www.westernsydney.edu.au/studysmart/home/digital_literacy/what_is_digital_literacy。

⁸² Andrew K. Przybylski博士等（2014年），“共同的责任 – 培养儿童网上复原力报告”（父母地带，牛津大学和维珍传媒，2014年），<https://parentzone.org.uk/sites/default/files/Building%20Online%20Resilience%20Report.pdf>。

教育工作者的工作因其工作环境和所施教的儿童和青少年（或成人）年龄组而有所不同。

性诱骗/网络性诱骗

根据卢森堡准则中的定义，性诱骗/网络性诱骗指面对面或通过互联网或其他数字技术与儿童建立/培养关系的过程，促成与该说服儿童发生性关系的人进行性接触或网上性接触⁸³。这是在儿童知情或不知情的情况下，引诱其进行性行为或带有性意味对话的过程，或涉及犯案人与儿童进行的、目的在于使儿童更易遭受性虐待的交流或社交的过程。性诱骗一词尚未在国际法中定义；包括加拿大在内的一些司法管辖区使用“引诱”一词。

信息通信技术（ICT）

信息通信技术指强调通信方面的所有信息技术。其中包括所有连接互联网的服务与设备，如计算机、笔记本电脑、平板电脑、智能手机、游戏机、电视和手表等⁸⁴。还包括无线电等业务，以及宽带、网络硬件和卫星系统等。

互联网及相关技术

现今，人们可使用多种不同设备与互联网连接，例如智能手机、平板电脑、游戏机、电视和笔记本电脑以及更传统的计算机。因此，除非上下文另有所指，否则对互联网的任何引用都应被理解为包含所有这些不同方法。为了涵盖互联网丰富而复杂的内容，“互联网和相关技术”、“ICT和网上行业”和“基于互联网的服务”可互换使用。

通知和撤销制度

客户、公众、执法机构或热线组织有时会在网上通知运营商和服务提供商有关可疑内容的情况。通知和撤销程序系指公司在得知其服务中存在非法内容（根据管辖区定义的非法内容）后，立即将其移除（“撤销”）的流程。

网络游戏

“网络游戏”的定义是通过任何连接互联网的设备（包括专用游戏机、台式计算机、笔记本电脑、平板电脑和移动电话）玩任何类型的单人或多人商业数字游戏。

“网络游戏生态系统”的定义包括通过电子竞技、流媒体或视频分享平台观看他人玩电子游戏，这些平台通常为观众提供评论或与玩家和其他观众互动的可选功能⁸⁵。

父母监控工具

指允许用户（一般为父母）控制计算机或其他可接入互联网的设备部分或所有功能的软件。通常，此类程序可限制访问特定类型和级别的网站或网上服务。一些工具亦提

⁸³ “保护儿童免受性剥削与性虐待卢森堡术语准则。”

⁸⁴ 儿基会和国际电联，《保护上网儿童行业准则》。

⁸⁵ 儿基会，“儿童权利与网络游戏：儿童和行业的机会与挑战，”系列讨论文件：数字世界中的儿童权利与工商业务，2019年，https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf。

供时间管理范围，即可设定设备仅在特定时段连接互联网。更高级的版本可记录设备发送或接收的所有文本。这些程序通常设有保护密码⁸⁶。

父母、看护人、监护人

多个互联网网站笼统地称为父母（如“父母网页”和“父母监控”）。因此，确定哪些人最适合让儿童最大限度地利用网上的机会，确保儿童和青少年安全及负责任地使用互联网网站，并同意访问特定的互联网网站，这可能是有益的。在本文中，“父母”一词指对儿童负有法律责任的任何人（教育工作者除外）。父母责任和父母法定权利则因国家而异。

个人信息

该术语指在网上收集的个人身份信息。其中包括全名、联系方式（如家庭地址和电子邮件地址）、电话号码、指纹或面部识别材料、保险号或任何其它能够实现与人面对面或网上联系或定位的要素。在此种情况下，该词还指由网上服务提供商在线收集的关于儿童及其随行人员的任何信息，包括联网玩具和物联网以及任何其他联网技术。

隐私

隐私通常通过以下方面衡量：网上共享个人信息，拥有公开社交媒体资料，与网上认识的人共享信息，使用隐私设置，与朋友共享密码，对隐私忧虑⁸⁷。

色情信息（Sexting）

色情信息通常定义为通过手机和/或互联网发送、接收或交换自制色情内容，包括图像、消息或视频⁸⁸。在大多数国家，制作、传播和持有儿童色情图像系违法行为。如果儿童色情图像公开，成年人不应观看。成人向儿童分享色情图像始终是犯罪行为，并且儿童之间可能出现伤害，需举报和采取行动删除分享的图像。

儿童性勒索或性敲诈

性勒索（也称为“网上性胁迫和勒索”⁸⁹）指“利用某人自拍的图像对其进行勒索，索取性好处、金钱或其他好处，威胁不经过被描绘者同意分享资料（如在社交媒体上张贴图像）”⁹⁰。

⁸⁶ 儿基会和国际电联，《保护上网儿童行业导则》。

⁸⁷ 儿童网上隐私保护法，Pub. L.，美国法典第15号6501-6505（1998年），<https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim>。

⁸⁸ “保护儿童免受性剥削与性虐待卢森堡术语导则。”

⁸⁹ 欧洲刑警组织，“作为一种影响儿童的犯罪形式的网上性胁迫和勒索：执法视角”（欧洲网络犯罪中心，2017年5月），https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf。

⁹⁰ “保护儿童免受性剥削与性虐待卢森堡术语导则。”

物联网 (IoT)

物联网指迈向社会和经济数字化的下一步，物品和人通过通信网络相互连接，并报告其状态和/或周围环境⁹¹。

URL

该缩写代表“统一资源定位符”，即互联网页面地址⁹²。

虚拟现实

虚拟现实指使用计算机技术创造互动三维世界的效果，其中物体具有空间存在感⁹³。

WI-FI

Wi-Fi（无线保真）是一组能够使数据通过无线网络传输的技术标准⁹⁴。

⁹¹ Ntantko, 物联网, 2013年10月1日, 数字化单一市场, 欧洲委员会, <https://ec.europa.eu/digital-single-market/en/internet-of-things>。

⁹² 儿基会和国际电联, 《保护上网儿童行业导则》。

⁹³ NASA, “虚拟现实”, [nas.nasa.gov](https://www.nasa.gov/Software/VWT/vr.html), 2020年1月16日获取, <https://www.nasa.gov/Software/VWT/vr.html>。

⁹⁴ 儿童网上隐私保护法。

附录2：针对儿童和青少年的接触犯罪

在互联网上，儿童和青少年可能会遇到一系列不必要或不适当的接触，这可能会给他们带来可怕后果。其中一些接触在本质上可能是性行为。

研究表明，22%的儿童遭到过网络欺凌⁹⁵、骚扰或跟踪；24%的儿童收到过不希望的性评论；⁹⁶8%的儿童在实际生活中遇到了之前他们只在网上知道的人⁹⁷。尽管不同国家和地区的比例数据各不相同，但这些数字表明，风险是真实存在的⁹⁸。美国的一项互联网研究⁹⁹发现，32%的网上青少年曾被完全陌生之人接触，其中23%的人表示，在接触时，他们感到恐惧和不安，4%的人说，他们遭遇过富有挑衅的性诱惑。

出于性目的，性侵犯者常常使用一种称为“grooming（诱骗）”的技术，利用互联网接触儿童和青少年。他们使用这种技术，通过勾起儿童的兴趣而获得儿童的信任。他们经常引入性话题、照片和大胆的语言，来麻痹青少年受害者、提高他们的性意识，并削弱其意志。性侵犯者利用礼物、金钱甚至交通票证，劝说和引诱儿童或青少年去往某个他们可实施性侵犯的地点。这些见面甚至被侵犯者拍照或录像。儿童和青少年往往情感欠成熟且缺乏自尊，这使他们容易受到操纵和恐吓。因窘迫或害怕失去互联网连接，他们还不愿意将其遭遇告诉大人。在一些情况下，他们遭到侵犯者的威胁，并被告知要保守这种关系的秘密。性侵犯者也通过互联网论坛和聊天室相互学习。

⁹⁵ U-报告（2019年）<http://www.ureport.in/v2/>。

⁹⁶ deSHAME项目（2017年），https://www.childnet.com/ufiles/Project_deSHAME_Dec_2017_Report.pdf。

⁹⁷ Lenhardt, A.、Anderson, M.、Smith, A.（2015年），青少年、技术与浪漫关系，<https://www.pewresearch.org/internet/2015/10/01/teens-technology-and-romantic-relationships/>

⁹⁸ Livingstone, S.、Haddon, L.、Görzig, A. 和 Ólafsson, K.（2011年），互联网上的风险和安全：欧洲儿童的观点。完整调查结果。伦敦政经学院：欧盟上网儿童，<http://eprints.lse.ac.uk/33731/>。

⁹⁹ Amanda Lenhart等人，“社交媒体的使用在青少年生活中获得了更大的立足点，因为他们接受了互动网上媒体的对话性质，”皮尤互联网与美国生活项目，2007年，44，https://www.pewinternet.org/wp-content/uploads/sites/9/media/Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf。

附录3：WeProtect全球联盟

WePROTECT国家响应模式

WePROTECT全球联盟战略支持各国在其国家响应模式（MNR）指导下，制定协调的利益攸关多方响应措施，以解决网上儿童性剥削问题。WPGA国家响应模式是国家行动蓝图，为各国解决网上儿童性剥削问题（OCSE）提供了一个框架。该模式旨在帮助各国：

- 评估其当前对OCSE的响应情况，并找出差距；
- 确定国家弥补差距工作的轻重缓急；
- 增进国际谅解与合作。

该模式不试图对活动做出规定或提出单一方式。模式的目的是描述有效保护儿童所需的能力，并支持各国开发或加强其现有能力。模式还列出一些促进因素，如果这些能够到位和有效，将加速和改善成果。MNR包括分为六个部分的二十一项能力：政策和治理、刑事司法、受害者、社会、业界和媒体以及沟通。WPGA认为，在所有六个领域采取行动将有助于国家对相关罪行做出全面响应。

该模式将使国家 – 无论其起点如何 – 能够发现能力上的差距，并开始计划弥补这些差距。虽然各国将制定各自的方式，但希望通过在共同商定的框架和对能力的理解范围内行事，国家和国际层面的利益攸关方之间的沟通与合作能够得到进一步加强。

WePROTECT全球战略响应

WePROTECT全球联盟全球战略响应（GSR）是打击网上儿童性剥削的协调方式，包括更强的全球洞察力、国家方式的国际协调以及超越国家主导响应机制的全球解决方案。本质上而言，GSR是国家响应模式（MNR）的配套手段；MNR侧重于在国家层面解决OCSE问题所需的能力，而GSR则重点关注国际合作和能力建设的优先领域。

GSR包括六个专题领域，每个领域都有相关的能力要求和预期成果，以及应跨境合作实现这些目标的合作伙伴。

政策和立法

形成采取行动的政治意愿并制定有效协调打击刑事犯罪方式的立法，将在国家和国际层面使相关高层不断做出打击网上儿童性剥削的承诺。

刑事司法

信息共享，包括通过正式的数据共享框架共享国际数据库，再加上在网上儿童性剥削方面具有专长的经过专门培训的官员和检察官，是识别、追查和逮捕罪犯的最佳方法，包括通过成功的联合调查和定罪手段。

受害人所受影响和服务

向受害者提供有效和及时的支持，包括保护他们的身份和给予他们发言权，这有助于确保受害者能够在需要时获得他们所需的支持。

技术

使用包括人工智能在内的技术解决方案来发现、阻止和防止有害材料、实时流媒体（直播）和网上诱骗（其中必须包括技术行业之间的广泛和一致的遵守执行），将方便相关平台避免被用作网上儿童性剥削的工具。

社会力量

在更广泛的社会中，有许多方面可协同工作，使儿童能够保护自己免受网上儿童性剥削，无论他们生活在何种地方。通过设计确保数字文化的发展更加安全（即内置安全功能），并确保媒体报道采取有道德和一致的方式，将会限制对网上非法内容的接触。与此同时，针对儿童和家长、看护人和专业人员的教育和宣传，以及针对罪犯的有针对性的干预，都有助于防止或减少网上儿童性剥削的发生。

研究与洞察

最后，威胁评估（如2019年全球威胁评估）、罪犯研究和了解长期受害者创伤的工作都将使政府、执法部门、民间团体、学术界和业界清晰了解最新威胁。

附录4：网上伤害响应示例

此处提供的示例由国际电联政策制定机构指南作者和相关撰稿人汇编。

教育孩子防范网上伤害

英国广播公司自有信息技术应用（**Own IT App**）是针对第一次收到智能手机的、8-13岁儿童福祉的应用程序。该程序将跟踪儿童在智能手机上活动的最先进机器学习技术与儿童自我报告情绪状态能力相结合，从而利用这些信息提供量身打造的内容和干预措施，帮助儿童实现快乐和健康上网。

该应用提供英国广播公司专门委托制作的内容 – 有用的材料和资源，帮助青少年充分利用上网时间，培养健康的上网行为和习惯，并帮助青少年与父母就其网上经历进行更有建设性的对话。该应用不会收集用户生成的任何个人数据或内容，因为整个机器学习都在应用内/用户设备内运行。

项目演进（**Project Evolve**）是一种资源充足的数字能力教育框架，可确定每个年龄段儿童的数字技能，帮助家长和教师了解他们的孩子应具备的能力，以及掌握特定技能所要求的资源和活动。

360度安全（**360 degree safe**）是一种自我评估工具，用于学校考虑和评估其整个上网安全规定，为获得确定的标准提供指导和支持。

DQ研究所（**DQ Institute**）– 数据收集自2017-2019年间30个国家的145 426名儿童和青少年（是由DQ研究所倡导的全球数字化公民运动#DQEveryChild的一部分）。该运动在新加坡启动，得到新加坡电信的支持，并在与世界经济论坛合作后迅速扩大，目前包括100多个合作伙伴组织。这一运动旨在通过在线教育和DQ世界评估方案，从孩子的数字生活开始就赋予他们全面的数字化公民能力。源自这一运动的数据被用以创建2020年儿童网上安全指数（**2020 Child Online Safety Index (COSI)**）。COSI框架根据影响儿童网上安全的六大支柱中的24个领域，对30个国家的儿童网上安全进行评估和排名。

DQ家庭获利就绪包（**DQ Pro Family Readiness Package**）和DQ世界（**DQ World**）为父母提供评估其子女数字就绪情况的机会，并通过教育材料提高数字能力，如数字化公民、屏幕时间管理、网络欺凌管理、网络安全管理、数字共情、数字足迹管理、批判性思维和隐私管理。

澳大利亚的学校电子安全工具包（**eSafety Toolkit for Schools**）是一套资源，旨在支持学校创建更安全的网上环境。该工具包反映上网安全教育的多方面方法，并被分为四个要素，其资源包括：

- 让学校做好准备，评估其处理网上安全问题的就绪情况，并提供旨在改进其当前的做法建议；
- 动员所有学校致力于并参与创建安全的网上环境；
- 通过强调网上安全教育的最佳做法进行教育，并支持学校开发学校界的网上安全能力；

- 在支持安全和福祉的同时有效应对事件。

波兰电子通信局-UKE的“我明智点击（I Click Sensible）”教育行动旨在教育儿童和父母如何更安全地上网，以及如何识别和管理风险。

越南儿童基金会（ChildFund Viet Nam）确立了安全刷卡（Swipe Safe）举措。该方案对儿童进行网上潜在风险教育，如网络诈骗、欺凌或性虐待，并提供有关保持安全的方法方面的意见和建议。

宽带委员会有关技术、宽带与教育的报告：推进全民教育议程（Technology, Broadband and Education: advancing the education for all agenda），2013年。

儿童上网体验：达成全球谅解和行动，儿基会，2019年。

全球上网儿童研究（Global Kids Online research）包括大量关于应对网上伤害的良好做法信息。

动员业界参与示例

澳大利亚eSafety专员与业界建立有强有力的伙伴关系并与业界合作，以对所有澳大利亚人进行赋能，使他们在网上获得更安全和更积极的体验，其中一个例子是eSafety在设计安全领域开展的工作。作为相关倡议的一部分，eSafety与负责保护用户的业界、贸易机构和组织以及父母、看护人和青少年进行了详细协商。“设计安全”倡议旨在鼓励和帮助业界确保将用户安全融入网上服务和平台的设计、开发和部署中。eSafety还管理三项举报和投诉机制：网络欺凌机制、基于图像的虐待机制和网上内容机制。eSafety可正式指示某些网上服务提供商从他们的服务中删除内容。尽管这些机制在很大程度上是作为政府和业界之间的合作模式运作的，但eSafety拥有的强制移除材料的权力为人们提供了重要的安全网络，并推动业界主动积极应对网络危害。

Telia公司负责了解和管理连接的负面影响问题，且在董事会层面是完全透明的和可追责的。他们也关心儿童和青少年，因为后者承认自己是他们服务的活跃用户。

波兰电子通信局-UKE（Office of Electronic Communications of Poland-UKE）正在动员民间团体和儿童参与其宣传活动，使他们认识到他们在网上签名的内容。

互联网观察基金会（The Internet Watch Foundation）是一个合作组织，将业界、政府、执法部门和非政府组织聚集一起，消除对儿童的性虐待。2020年，IWF有152个跨平台和基础设施服务成员，并向成员提供一系列服务，以防止在其平台上传播犯罪图像。

立法的覆盖范围

通过签署《上网儿童安全世界宣言》（Child Online Safety Universal Declaration）（宽带委员会）表达优先开展保护上网儿童（COP）工作的政治意愿。

监管

《经济学人》情报部的《走出阴影：关注关于儿童性虐待和剥削的响应指数》（2019年）是分析各国应对儿童性虐待和性剥削的唯一基准工具，包括数字空间和ICT行业做出的响应。

识别网上虐待儿童行为

以下是识别网上虐待儿童行为的良好做法示例。

INHOPE: INHOPE（国际互联网热线协会）网络建立于1999年，旨在打击网上CSAM，以实现人们的没有儿童性虐待材料的互联网的共同愿景。在这期间的20年中，INHOPE成功遏制了网上CSAM的增长、地理传播和严重性。如今，INHOPE热线在各大洲良好运行，接收举报并迅速将CSAM从互联网上移除，同时与执法部门共享数据。

微软PhotoDNA可创建图像的哈希值（hashes），并将这些值与已识别并确认为CSAM的哈希值数据库进行比较。如果发现匹配，则图像将被阻止。然而，该工具不采用面部识别技术，也不能识别图像中的人或物体。但是，随着视频PhotoDNA的发明，情况已出现新的转机。

视频PhotoDNA将视频分解成关键帧，并为这些截屏创建哈希值。就像PhotoDNA可匹配为避免被发现而被篡改的图像一样，视频PhotoDNA可找到被编辑或拼接成视频的儿童性剥削内容，若非如此这些内容可能看起来根本无害。

微软发布了一款新工具，用于识别在网上聊天中为进行虐待而诱骗儿童的性侵犯者。**阿尔特弥斯项目（Project Artemis）**是与Meet Group、Roblox、Kik和Thorn合作开发的，以微软的专利技术为基础，将通过Thorn免费提供给提供聊天功能的网上服务公司。阿尔特弥斯项目是一款技术工具，当聊天室需要任何节制时，可帮助向管理人员发出危险信号。这一诱骗发现技术将能够发现、定位和报告试图以性为目的引诱儿童的性侵犯者。

Thorn开发了针对搜索儿童性虐待内容的震慑性广告，在三年的时间里，这类广告在四个搜索引擎上被搜索了数百万次。此外，在搜索性剥削材料后，寻求帮助的人们对这些广告的点击率达到了3%。

Thorn更安全（Thorn's Safer）是一款可直接部署到私人公司平台上的工具，用于识别、移除和报告CSAM。

Thorn Spotlight这一软件使美国所有50个州和加拿大的执法部门能够加快识别受害者，并将调查时间缩短60%以上。

Geebo是一个致力于在其平台上杜绝性剥削的分类网站，从未有过涉及儿童性剥削的案例。他们之所以能做到这一点，部分原因是他们建立有预筛选程序。

谷歌人工智能分类器（**Google AI classifier**）可用于发现网络、服务和平台上的儿童性虐待材料。该工具可通过谷歌内容安全应用程序接口（**Google Content Safety API**）免费获得。这一工具包能够以更少的人可接触到它的方式提高内容审查能力。这一工具将帮助真人专家更大规模地审查材料，并通过锁定以前未被标记为非法材料的图像跟踪罪犯。分享这项技术将加速图像的识别。

2015年，谷歌扩大了哈希方面的工作，为**YouTube**上的视频引入了首个指纹识别和匹配技术，该技术可扫描并识别上传的包含已知儿童性虐待材料的视频。

在2019年儿童安全黑客马拉松（Child Safety Hackathon）比赛期间，**脸书**宣布开放两项技术的源码，这些技术可检测出完全相同或几乎完全相同的照片和视频。这两种算法在GitHub中提供，方便哈希共享系统相互通信，从而使系统更加强大。

IWF热线始终保持警惕，不仅对来自公众的数千份报告予以跟进（公众可能偶然发现了网上的儿童性虐待图像），而且还发挥了独特的在网上搜索这种非法内容的积极主动作用。通过赋能热线利用其信息和重点资源的能力，更多的内容可被识别和删除。此外，IWF一直在与谷歌、微软、脸谱和其成员范围内的其他公司合作，以不断突破技术界限。IWF提供报告门户（[Reporting Portal](#)）解决方案，方便没有热线的国家的互联网用户通过定制的网络门户页面直接向IWF举报涉嫌儿童性虐待的图像和视频。

IWF与受害者支持慈善机构玛丽·科林斯基金会（Marie Collins Foundation）合作，旨在发起新的行动，呼吁年轻男性举报他们在网上浏览时可能无意中发现的、任何自己制作的18岁以下儿童的性图像或视频。

国际刑警组织建立了国际儿童性剥削（ICSE）图像和视频数据库——一项情报和调查工具——方便来自50多个国家的专业调查人员分享儿童性虐待案件的数据。通过分析照片和视频的数字、视频和音频内容，受害者鉴定专家可检索线索，识别案件中的任何重叠之处，并共同努力寻找儿童性虐待的受害者。目前，国际刑警组织儿童性剥削数据库保存有150多万张图像和视频，并在全世界帮助确认了19 400名受害者。

NetClean ProActive是一款基于签名匹配和其他检测算法的软件，可自动发现企业环境中的儿童性虐待图像和视频。

格里菲耶大脑（Griffeye Brain）使用人工智能扫描以前未予分类的内容，将其与已知CSAM内容的属性进行比较，并对可疑数据内容做出标记，供代理审查。

RAINN与全国1 000多家地方性攻击报告服务提供商合作，创建并运营国家性攻击热线，并为国防部运营国防部安全帮助热线。RAINN还开展防止性暴力、帮助幸存者并确保罪犯被绳之以法的项目。

Safehorizon是受害者援助非营利组织，自1978年以来一直支持纽约市的暴力和虐待受害者。Safehorizon为暴力受害者提供热线服务。

Project Arachnid是Project Arachnid加拿大中心运作的一项创新工具，旨在打击互联网上日益泛滥的儿童性虐待材料（CSAM）。

^[1] <http://www.oecd.org/internet/bridging-the-digital-gender-divide.pdf>

支持机构：



国际电信联盟

Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-30455-3



瑞士出版

日内瓦, 2020

图片来源: Shutterstock