IGF 2018 关键信息——网络安全，信任和隐私

总体信息

所有利益相关者都认同网络安全的重要性和相关性。只有安全可靠的网络空间才能产生和维护人们对互联网的信任。随着互联网和新技术的发展，网络安全问题越来越复杂，涉及的角度和问题越来越多，涉及的主体也越来越广泛。隐私、数据保护和新技术的安全性是网络安全对话的核心问题之一。

信任和利益相关者的合作

- 网络安全和隐私往往是相互交织和相互依存的，它们会影响人们对数字空间的信任，并可能限制其增长和繁荣的潜力。基于政府、私营部门、技术社区和民间团体相互承认和良好的参与模式的合作，可以在不损害互联网开放、自由和安全性质的前提下解决隐私和网络安全问题。

- 关于网络安全的整体观点，涉及国家和组织内的技术和经济、社会、文化因素很重要。风险管理和多利益相关者的流程对于开始对话、共同工作和建立信任至关重要。

- 多方利益相关方合作加强网络安全能力建设被视为一项重大挑战。政府部门、私营部门和民间团体之间的联合参与应成为更有效、更有力和可持续的公私伙伴关系的基础。

- 安全是所有涉众的任务，包括个人用户。当可以意识到风险和意识到他们行为的知情用户活跃在互联网时可以做出更好的决定。然而，通常情况下，

终端用户被视为风险或威胁的一部分，他们承担了太多的责任，而网络安全措施应该侧重于保护所有人。

网络外交

- 网络稳定是国家和非国家行为者的共同目标。如果没有稳定的网络，网络空间的利益和数字经济的未来将受到危害。利益相关者需要认识到网络威胁的高度复杂性和跨界性，并开展适当的国际合作，共享信息，追求负责任的行为准则。

- 把外交努力和建立信任的措施相结合可以有助于防止国家间的网络冲突，而不具约束力的网络空间，国家行为自愿规范建设则是必不可少的指南。

- 各国在确保网络稳定方面负有法律和道德责任。政策提案、对网络武器扩散的控制，以及对保护互联网公共核心的承诺，都有助于网络稳定。

- 制定网络安全战略需要多方利益相关者和多学科的方法。虽然所有人的共同利益都是需要有一个稳定和安全的网络空间，但每个利益攸关方都有自己的、但相辅相成的责任。

- 网络空间与现实世界是不同的，但并不是独立的。因此，我们应该把构成世界和社会基础的现有原则，与应对网络空间固有挑战的具体对策结合起来，作为互联网治理的基本原则。

数据的隐私和保护

- 北半球的国家为协调保护隐私和获取数据以应对数字威胁而采取的制度影响了整个互联网生态系统，因此可能对南半球国家产生影响，这样就有机会以相互同意和协商的方式在发达国家和发展中国家之间建立法律互操作性框架。

- 想要加强数字身份管理必须增加数据的隐私性，特别是在国家数字身份计划强制要求进行数据共享的情况下。必须保护个人资料不受黑客入侵和滥用，同时避免追踪和监控用户。

- 生物特征数据也是隐私数据，需要最低程度的保护。生物特征信息与人及其生命有着不可分割的联系，并且可能存在被滥用的风险。安全、尊重权利地使用生物识别技术需要不同背景(如技术、商业、政府、哲学、性别专家等)的专家、从业者和利益相关者的合作。
- 隐私权是个人自由生活、形成观点、无所畏惧地表达自己、充分发展个性的重要保障。对于社会中处境最不利和最易受伤害的成员来说，隐私保护是关键，因为他们更容易受到歧视。隐私保护对于公民社会的运作和有意义地参与公共生活至关重要。

- 继续推动有意义的访问是在新的数字鸿沟的背景下进行的。在新的数字鸿沟中，保护隐私需要付出巨大的经济代价，并可能削弱人们选择排除的能力。

- “智慧城市”将日益改进城市治理和公共政策。在个人资料的使用和保护方面需要有洞察力，以及可能存在的法律空白会导致无意的社会和经济歧视，也包括在获得公共服务方面的歧视。

算法

更好地理解算法如何影响人们的生活，理解自动化的口译算法决策所存在潜在风险，以及它们对人权和隐私权的影响，会使我们有足够的技术和政策解决方案，以及解释的权利。

物联网

物联网是数字革命的关键驱动力，它为我们的社会创造了新机遇，比如新产品和新服务，但同时也带来了脆弱性。网络安全是信任物联网的基本要求，因为一个漏洞就可能会破坏个人用户和整个社会的信任。由于物联网是一种跨国界的产物，因此需要一种全球或区域的联合方式。

仇恨言论

仇恨言论和自由表达不受欢迎的意见之间的区别可能很复杂。删除相关内容是一项重要的挑战，而且这并不能完全解决问题。与仇恨言论相关的挑战需

要一种全面的方法。需要有一个利益攸关方进行教育和合作，开发赋予公民权力的工具和新的报告制度。

法律和监管问题

- 企业必须保护自己免受数字环境中成倍增长的多数量和多种类的威胁，但也要依靠政府对攻击者采取法律反攻行动。公共政策应进一步演变和澄清私营部门主动防御措施的条件、限制和保障措施。

- 鉴于立法速度往往难以跟上网络安全领域变化的步伐，网络安全规范可作为国家和非国家行为体就网络空间中负责任行为达成一致的重要机制。

- 社交平台巨头和政府都认识到监管的必要性。重要的是加强监管过程中的合作，并让多方利益相关者充分参与，以使监管有效和可执行。风险管理措施也应该被收入到法规中。监管的公私伙伴关系可以成为一种解决方案，为各国争取政治上的支持和可预测性，并为科技公司的经济盈利能力提供保障。“要么接受，要么放弃”的办法是没有帮助的，因此，需要更多的资源和努力，以有效的方式推动联合管理进程。

网络安全最佳实践

- 网络安全战略开发和实现协作模式的成功实现依赖于所有参与者之间的敏捷适应性、透明性和可信信息的共享性。网络安全合作应显示利益相关者之间的纵向和横向的合作，应具有描述性而非说明性，并应足够敏捷，以适应不断发展的网络风险和技术。参与者不仅应扩大到拥有和控制关键信息基础设施的公共和私营部门实体，而且应该吸纳其他行业利益相关者(例如,银行和金融行业,业务流程外包(BPO)、健康、旅游、和能源领域)和非营利组织的利益相关者群体(如技术社区,学术界和民间团体)。

- 网络安全领域的政府和社会资本合作 (PPPs) 应使政府和主要互联网服务商 (ISPs) 能够汇聚资源和技术，以应对网络安全的关键问题，包括保护关键

基础设施和打击网络犯罪。公营和私营部门打击网络犯罪的有效合作经常受到不同的挑战，比如披露和曝光、多变的责任和监管环境、跨境数据传输限制和网络犯罪调查。

- 重要的是，各国应通过基于风险的方式实施国家网络安全措施。网络安全决策必须考虑到数字环境提供的社会和经济机会，同时也要保障基本权利。在网络安全、经济发展和人权之间实现动态平衡，需要的答案不仅限于严格旨在消除这种威胁的技术解决方案。相反，为了获得数字化的社会和经济效益，在保护基本价值观的同时，利益相关者必须将风险降低到可接受的水平。

- 利益攸关方应在基于风险框架的条件下促进加强区域和国家网络安全倡议的协调与协作。在建设国家和地区网络安全能力方面，采取更有意义的全球导向方式和更基于战略风险的合作方法，这将会使各国能够灵活应对安全挑战。

- 网络安全威胁影响到政府、私营企业和普通民众。一般来说，准则对于不同的方面以及世界各地都是有益的，但是需要做出更多的努力使非国家利益攸关方参与准则的制订和执行。

*这是向社区投入开放的*IGF*消息的初稿。如需提供信息反馈，请写信至*igf@un.org*