Publication: Lianhe ZaoBao, p 28
Date: 26 October 2017

Headline: Protect our digital life 保卫我们的数码生活

狮城脉搏 陈庆文

保卫我们的数码生活

作为一个高度连接的社会，来自网络世界的威胁已逐渐重新定义我们的国家安全。网络攻击已从非传统安全威胁演变成包括谍报、欺诈和破坏的激烈冲突新领域。物联网（Internet of Things）的脆弱性能造成实际的损害。

随着我们的网络基础设施日渐庞大，要对抗多层面又快速变化的威胁，网络安全是一个迫切需要多方利益相关者进行探讨的领域。

研究、维持和加强网络防卫能力，绝不能只是政府的专利。在跨国际的网络空间，通常涉及国家行为体（state actors）的网络威胁也意味着，国际合作和值得信赖的合作伙伴之间的情报共享，将显得更加重要。这同时需要跨政府和跨领域的进一步努力。

为了辅助美国军人和科学家的模拟通信，互联网应运而生。在这样的机制里，信任是最重要的基础。

人们互相沟通，相信彼此所言，所传达的讯息也会根据现有的法律和社会规范进行处理。

今天，无论是工作、经济、休闲、军事行动或教育，我们都依赖互联网。然而，作为最基本元素的信任，却是四面楚歌。

从在线个人监控、黑客入侵、企业和政府的间谍活动、互联网流量劫持，再到遥控工业、政府和军事用途的电脑，今天的互联网使用者面对着各种各样的网络攻击。

很多时候，在匆忙地开上网络的高速公路之际，不管是心脏起搏器、汽车或家庭保安摄像机，都忽略了安全性，不然就是在原初的设计中，因不被视为重要的环节而将之推迟。然而，这些新兴科技和新联网设备的安全措施若不足或差劲，将会严重冲击商业和社会。

网络攻击所带来的巨大危险性绝不能被低估。公众的恐惧和惊慌，加上若对公共设施、地铁系统、医院运作、云计算和电子银行交易，这些我们常常理所当然地视为安全及可靠的事物失去信任，将对我们的生活造成无法估计的破坏。

在许多例子中，个人隐私、知识产权、专有数据、机密资料曾被滥用、侵占或作为非法用途。为了让公共服务的电脑网络更为安全，新加坡政府在2016年6月实行了前所未有的举措，宣布从2017年5月起，公务员用来电邮的电脑将不能上网。

简而言之，互联网作为一个可靠、安全和开放性的基础设施，其可靠性正遭受尤其是来自恐怖主义的巨大威胁。经济、公共设施和交通等不少系统，都得依赖互联网才能有效地运作，发挥效能。随着坏境的改变进行调整是非常关键的。

当有情报显示，即将发生的网络攻击可重创公用事业、电信、金融和交通系统等重要基础设施时，已经修正的新加坡法律赋予了有关当局先发制人的权力，以应对这类威胁。一个挑战是公众似乎对这个真实而迫切的危机完全浑然不觉。

从根本上来说，网络安全面对的是保安、经济和政治方面的挑战。即使我们专注于采用先发制人的手段应付威胁，我们还是得加强整体的安全架构，以确保在面对真实而燃眉的危机时，我们的反应是快速而适当的。

在网络攻击发生后，我们的重要基础设施和整体的应对措施都必须具备韧性，好让我们的社会能安然无恙地回弹，迅速恢复正常。反应不足所造成的破坏，远比安全漏洞本身来得大。

坚韧性绝不只是拥有一套业务连续性计划（编按：BCP，指灾难发生后保持运作的能力）。我们的社会是否承受得了先进的网络攻击而不会陷入瘫痪状态，以致大家在生活中的通信条件因此退化？

在新的网络环境，我们共同的数码未来，取决于多方利益相关者在本地和国际的牢固合作关系。威胁的规模和复杂性难免会让人觉得无助和绝望，因而使问题加剧。这转而影响了不同的利益相关者以互惠互利的方式，进行合作和投资的意愿。

协调不同的利益

不过，在一个日益数码化和一体化的世界，没有人能独善其身。2014年，麦肯锡（McKinsey）估计到了2020年，云计算将能创造3.72万亿美元（约5.11万亿新元）的价值。不过它警告："在一个网络攻击变本加厉的环境里，人们对公共云（public clouds）的脆弱性日感担忧，另外，为了遵守第三方机构使用数据以及系统的更严格条例所导致的更高昂费用，公共云将因此无法物尽其用。这些问题将会对许多系统的采用造成拖延，并会使云计算的潜在价值减少多达1.4万亿美元（约1.9万亿新元）。"缺乏信任，影响是既深且广。

恐怖分子正利用网络空间作为沟通工具，招募新血和召集他们的支持者，甚至提供技术支援。

同样的，暗网（编按：Dark Web，需要特殊软件才能登录的互联网）是犯罪活动的渊薮，利用不断推陈出新的隐身软件，非法活动大行其道。就像贩卖毒品、武器和其他非法商品及服务，而于2013年被查封的网上黑市"丝绸之路"（Silk Road），即使执法当局将一个主犯绳之以法，很快就有其他黑市交易网站取而代之。

因此，当务之急是调节表面上相互竞争的各方利益，以制定一致和综合的应对措施。由于网络空间存在着"公地悲剧"（编按：tragedy of the commons，指三不管地带），利益相关者总假定第三方，这里通常是指政府，会保护网络空间的安全、抵挡网络攻击、进行风险监测、制定应急计划和恢复正常秩序，从而令这项工作充满挑战性。

然而，研究、维持和加强网络防卫能力，绝不能只是政府的专利。在跨国际的网络空间，通常涉及国家行为体（state actors）的网络威胁也意味着，国际合作和值得信赖的合作伙伴之间的情报共享，将显得更加重要。这同时需要跨政府和跨领域的进一步努力。

鉴于网络安全的稳固程度只能取决于它最薄弱的环节，政府得持续加强公共教育和宣传，让每个人和每个机构都知道在提升网络安全方面所需扮演的角色。

今天的网络环境为革新、交流、商业和创意提供了无限的机会，但拥有这些好处的同时，也带来了严峻的安全挑战。要找到令人满意的解决方法，须要公共和私人机构建立具持续性的伙伴关系，为促进信息的定期分享和集体防御，制定机制和奖励方式，以及教育利益相关者，在挫败日益复杂的攻击所身负的角色。

网络攻击日益增加，我们在着力追求更高连接性的当儿，绝不能让对我们的生活素质和方式如此重要的互联网成为"特洛伊木马"（Trojan horse）。

作者是新加坡管理大学法律系副教授
早报言论组译

Source: Lianhe ZaoBao @ Singapore Presss Holdings Limited. Permission required for reproduction