网络安全

1988年，互联网的公共使用尚属初期阶段，因此该年度制定的《国际电信规则》（ITR）未明确包含有关网络安全的条款，但针对当时首次传播的一款恶意软件 – 莫尔斯蠕虫，《规则》（第9条）规定应避免“技术危害”。自《规则》问世以来的几十年间，保护网络安全的重要性极大地得到加强，并将在审议ITR时得到考虑。目前相关国家已提出提案，建议在该条约中增加或修正与安全有关的内容，包括打击垃圾信息的措施。

网络攻击的数量和复杂程度与日俱增，而同时我们又在更多地依赖互联网和其它网络获取关键性服务和信息。MCAFEE安全公司的研究表明，2011年是发现（网络）威胁数量最多的一年。据称该年度在世界范围传播的恶意软件至少达到了7 000万款，且智能电话已成为这些恶意软件传播的手段。分析人士的报告称，至少70%的电子邮件是垃圾邮件。

与此同时，智能电网、云计算、工业自动化网络、智能交通系统、电子政务和电子银行等诸多类型基础设施日益实现互连，呈现一损俱损的局面。网络为人们带来更多便利和更高效率的同时，也使人们在网络攻击 面前更加不堪一击。[1]

尽管如此，目前尚未制定在全球范围令人接受的网络安全定义，阻碍了网络保护工作的开展。鉴于现今网络和计算机系统没有边界，因此必须在国家和国际层面解决这一问题。

与信息通信技术（ICT）相关的事件通常在现有国家刑法（不能经常得到更新或与全球趋势同步）框架内处理，我们尚未制定此方面相关犯罪的通用国际标准：例如，是否应包括软件盗版和儿童色情？财务欺诈以及拒绝服务攻击？对这些问题的答案或许可以是统一国内法律，并确立可实现国际合作的法律框架。然而有些人认为，这种工作并非必要，或认为仅应在区域层面开展这一工作。

法律并非是应对网络攻击的唯一或最迅速的武器，可通过能够实现互操作性和符合安全措施要求的标准对技术解决方案予以补充。在当今相互依存的网络世界中，这一点尤为重要。国际电联电信标准化部门（ITU-T）已发布了300多项与网络安全有关的标准，且国际电联正在协助发展中国家开展此领域工作，支持它们建立计算机事件响应组 – CIRT。国际电联在其《全球网络安全议程》[2]中倡导开展国际合作。

在2003和2005年举行的信息社会世界峰会上，世界领导人赋予国际电联领导“树立使用ICT的信心和加强安全性”的国际协调任务，因此该项工作是国际电联职责的一个组成部分。

---

[1] 亦见有关“保护关键性国家基础设施”的WCIT背景简介。

[2] 见“www.itu.int/osg/csd/cybersecurity/gca/”